УДК 007:004.56:351.824.11(824.11(477)+007.004.56:005.334(477) **DOI 10.33042/2522-1809-2020-3-156-80-87**

М.Д. Василенко, О.Б. Козін, М.О. Козіна, В.О. Рачук

Національний університет «Одеська юридична академія», Україна

КІБЕР-РИЗИКИ В МУНІЦІПАЛЬНОМУ ГОСПОДАРСТВІ В ПЕРІОД ПАНДЕМІЇ: ЗБИТКИ ТА БОРОТЬБА ЗА КІБЕРБЕЗПЕКУ

В статті проаналізовано дистанційне управління та автоматизація інфраструктури муніципального господарства, які є вразливими для вторгнень, атак, людських помилок, нещасних випадків, що збільшуються. Представлені результати вивчання нових кібер-ризиків муніципального господарства, що виникли у період пандемії, формулюється власний погляд щодо їх класифікації та методів протидії з боку муніципальних організацій та підприємств.

Ключові слова: *кібер-безпека, кібер-ризик, муніципальне господарство, "фішинг", пандемія, Covid-19.*

Постановка проблеми

Не викликає ніяких сумнівів, що сучасне місто представляє собою складну соціально-економічну систему з розвинутою інженерною інфраструктурою з багатьма значущими елементами. Місто включає в себе системи водо-, електро-, тепло-, газопостачання; каналізацію; підприємства житлово-комунального комплексу, підприємства сміттєвидалення і переробки міських відходів та ще багато інших структур (підприємств) (див. [1]). Саме в містах існує достатня кількість таких підприємств (комунальних), а в великих містах (м. Київ, м. Харків, м. Одеса та інші) існують десятки комунальних підприємств. Так, з інформації Одеської міської ради в м. Одесі обліковано 45 комунальних підприємств. Робота майже усіх з них, як і робота комунальних підприємств в інших містах, пов'язана з певними ризиками. При цьому практичне керування ризиками та вміння застосувати теорію ризиків на практиці дає позитивний ефект в діяльності з уникнення або мінімізації наслідків ризиків. В цілому з позицій комунального господарства «ризик» можна конкретизувати як «відхилення фактичного результату від очікуваного», то як «ймовірність певної небажаної події». Наразі не існує однозначного тлумачення терміну «ризик» [2]. Деякі питання розуміння ризиків від правової до інформаційної складових обговорювалися в роботі [3] з участю авторів цієї праці. В складних системах, до яких належить комунальне господарство міста, використовуються ймовірнісно-статистичні методи. Відомо, що ці методи використовують прогнозування в таких галузях як економіка, політика, психологія та ін., тобто для складних систем, що перебувають під впливом численних факторів [4, с. 475]. Саме в цих випадках найбільш важливим стає саме ризик, що підкреслює, що ризики передбачити складно, оскільки прогнозування сукупності підприємств комунального господарства не є об'єктивною категорією, що не скажеш про ризики.

Згадуючи муніципальне господарство зазначимо, що економіка сучасних муніципальних структур міста в даний час взаємопов'язана з віртуальними електронними мережами, базами даних й конфіденційною й транзитною інформацією. В результаті дистанційного управління та автоматизації інфраструктури муніципального господарства стає надзвичайно вразливою для вторгнень, атак, людських помилок, нещасних випадків, які збільшуються, незважаючи на постійну роботу професіоналів – ризик-менеджерів. Через концентрацію комп'ютерних операційних систем і програмного забезпечення «кібер-ризик» муніципального господарства носить мультиплікативний характер, що робить його системним і міжнародним. Його сутність проявляється як на національному, так і на глобальному рівні шляхом впливу на бізнес, муніципальні органи і органи державної влади. З огляду на численність і витонченість наявних ризиків доцільно забезпечити високий рівень кібербезпеки. При цьому наявна пандемія сприяє підвищенню кількості кібер-атак, що свідчить про підвищену актуальність щодо кібер-уразливості адміністрацій муніципальних органів й органів державної влади.

Аналіз останніх досліджень та публікацій

Питання менеджменту в системі управління міським господарством досліджено досить ретельно. Тому звернемо увагу на посібник, який включив в себе базові положення з цих питань, поєднав теоретичні основи менеджменту та методи їх практичного використання в діяльності організацій

міського господарства [5]. Однак щодо кібер-ризиків в комунальному господарстві міста, нажаль, автори не встановили достатню кількість праць, де ці питання обговорюються. Так, в роботі [6] визначено та класифіковано ризики в житлово-комунальному господарстві з висновком, що управління ризиками житлово-комунального сектора можна розглядати як важливий аспект забезпечення стійкості галузі, який потребує всебічних досліджень. Ризик та його стадії в економіці становили предмет дослідження таких економістів, як: Ф. Найт, Г. В. Чернова, А. А. Кудрявцев, Л. І. Донець. При цьому немає сенсу наводити усю сукупність робіт з цього питання, посилаємося лише на ті, що привернули нашу увагу [6-8]. Часто в роботах економічного характеру під ризиком розуміється можливість (ймовірність) виникнення умов, які призведуть до негативних економічних наслідків. Функціонування ризиків у форматі ринкових відносин характеризується неповною інформаційною відкритістю та наявністю протиріч. Такі ризики є стохастичними за своєю суттю. В таких випадках важливо враховувати вплив ризику, коли негативними наслідками можуть стати втрата частини ресурсів, недоотримання доходів, поява додаткових витрат, збитки, закриття інвестиційних проектів тощо. Тут ризик стає тісно пов'язаним з настанням ризикових ситуацій, тобто з сукупністю подій (обставин) і умов, що створюють обстановку невизначеності, яка може як сприяти, так і перешкоджати досягненню цілей. Невизначеність обумовлює наступ ситуації, яка не має однозначного результату, і тому якщо існує можливість кількісно і якісно визначити ступінь ймовірності появи того чи іншого варіанту, це і буде ситуація ризику. У роботі [8] наведені результати аналізу вітчизняної та зарубіжної літератури за темою методів оцінки ризиків кібербезпеки, у тому числі об’єктів критичної інфраструктури. У роботі запропоновано графічний та аналітичний методи оцінки сумарного ризику кібербезпеки інформаційних систем, у тому числі об’єктів критичної інфраструктури.

Мета статті полягає у визначенні, на засадах системного аналізу, нових кібер-ризиків муніципального господарства, що виникли у період пандемії, формулюванні власного погляду щодо їх класифікації та методів протидії їм з боку муніципальних організацій та підприємств.

Виклад основного матеріалу дослідження

Зазвичай кібер-ризики розглядаються разом із заподіяними збитками. За оцінками експертів з кібербезпеки Cybersecurity Ventures підраховано, що кібер-вимагачі в 2019 році переслідували інститути муніципальних та державних органів влади, а також бізнес кожні 14 секунд. До 2021 року цей інтервал повинен зменшитися до 11 секунд. За прогнозом Всесвітнього економічного форуму, сума планетарного збитку від кібератак до 2022 року, може вирости до 8 трлн. доларів [9, 10]. Оскільки базова технологія стає усе більш складною, ми стикаємося з новими проблемами кібербезпеки, які вимагають більше часу і навичок для відвертання і лікування. Впродовж 2019-1920 років ситуація з кібер-вимагачами залишалася і залишається дуже напруженою, і хакери продовжують атаки, орієнтовані, в основному, на муніципальні та державні органи влади, уряд та бізнесові структури. Так, спостерігається збільшення числа хакерських атак, що використовують уразливості видаленого доступу для діставання цільового нелегального доступу без втручання людини, окрім фішингових операцій, з метою перетворення їх в додаткові можливості для отримання викупу.

Згідно з даними, опублікованими Центром скарг на інтернет-злочини (ЦСІ3) ФБР (США) у звіті про злочинність в інтернеті за 2019 рік, злочини і шахрайства з використанням Інтернету не мають ніяких ознак, щоб говорити про їх припинення. Так, в США за останній рік було зареєстровано як найбільшу кількість скарг, так і найбільші втрати з моменту створення центру в травні 2000 року. ЦСІ3 отримав 467 361 скаргу в 2019 році - в середньому близько 1300 щодня - і зафіксував збитки у розмірі більше 3,5 мільярдів доларів для приватних осіб і постраждалого бізнесу [11]. Великі багатонаціональні корпорації, а також муніципальні та регіональні органи влади США використали в 2019 році не менше 170 млн. дол. США для покриття витрат на викуп. Це включає витрати на розслідування самої атаки, відновлення комп’ютерних систем за допомогою резервних копій, відновлення інфраструктури, виплату викупу, якщо це необхідно, і вжиття превентивних заходів для відвертання повторення подібних подій [11].

У даної роботі автори зосередили увагу на атаках на основні складові муніципальних та державних органів влади, не вдаючись до подробиць атак на окремих осіб, що також є достатньо великою кіберзагрозою у світі.

Розглянемо деякі з основних глобальних кібер-атак вимагачів, які уразили підприємства та міста на прикладі міст і штатів США в 2019 році. Загальновідомо про скоординовану атаку на міста штату Техасу (США) [12, 13]. В 22 містах Техасу 16 серпня 2019 р. була проведена скоординована атака вимагачів з використанням шкідливої програми REvil (Sodinokibi). Муніципалітети були виключені зі своїх IT-систем після того, як хакери зламали програмне забезпечення від стороннього постачальника послуг, який видалено управляв їх

ІТ-інфраструктурою. Хакери вимагали викуп у розмірі 2,5 мільйонів доларів, але ніхто не заплатив. Ці міста перейшли від оцінки до відновлення, понісши як мінімум 12 мільйонів доларів збитків, включаючи витрати влади графств, освітніх установ та міст [12, 13]. Тут також доречно відзначити атаку вимагачів у м. Балтімор, коли були зіпсовані комп'ютерні програми щодо забезпечення життєдіяльності міста [14, 15, 16]. Так, деякі критично важливі функції були зловмисно зашифровані таким чином, що комп'ютерні системи міста піддавалися впливу вірусу-здирника, відомого як RobbinHood. Збиток поширився на послуги онлайн-оплати рахунків за воду, системи електронної та голосової пошти муніципальних службовців, електронні звернення в мерію, продаж нерухомості, податки на майно і дорожні котирування, операції з нерухомістю, онлайн-оплати штрафів і багато іншого. Були пошкоджені бази даних майже усіх комунальних систем. В результаті виявилося неможливим проводити будь-які дії з рахунками на оплату, виготовляти та отримати різноманітні документи, наприклад, документи про відсутність комунальних заборгованостей громадян, що продають або купують нерухомість і т.д. [17, 18]. Пірати запропонували владі місцевого самоврядування внести викуп у розмірі 76 000 доларів на обмін на ключ для розшифровки. Місцева влада відмовилася та відновила дані та програмне забезпечення систем самостійно, витративши 18,2 млн. дол. США. Гроші були витрачені на відновлення, судовий аналіз, виявлення, нове апаратне і програмне забезпечення та розгортання нових систем.

Нові проблеми з'явилися майже у всіх владних структурах у світі з появою COVID-19 (коронавірусу). Урядові рекомендації, що стосувалися COVID-19, майже у всіх країнах привели до безпрецедентного переходу всіх муніципальних і державних установ на телероботу. Проте також важливо було вжити необхідних заходів для забезпечення того, щоб муніципальні організації залишалися захищеними від кібер-ризиків в цих виняткових обставинах. Для забезпечення безперервної діяльності безпечним чином інституції та приватні особи мали проявити й майже у всіх випадках проявили зацікавленість в оптимізації віддалених операцій. В таких випадках проявляють активність і почитають свою руйнівну роботу фішингові кампанії. Як загальновідомо фішинг представляє собою різновид інтернет-шахрайства, метою якого є діставання доступу до конфіденційних даних користувачів - логінів і паролів. Це досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень усередині різних сервісів, наприклад, від імені банків або усередині соціальних мереж. У листі часто міститься пряме посилання на сайт, зовні невідмітний від сьогодення, або на сайт з редиректом. Після того, як користувач потрапляє на підробну сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробній сторінці свої логін і пароль, які він використовує для доступу до певного сайту, що дозволяє шахраям отримати доступ до аккаунтів та банківських рахунків. У той час як сьогодні в багатьох містах та установах запроваджувалися заходи, щоб допомогти жертвам COVID-19 і обмежити зараження, хакери використовували кризу і продовжують свої дії для здійснення цілеспрямованих кібератак на підприємства, зокрема, на робочі місця. У період кризи хакери намагаються використовувати увагу, яку приділяють вірусу, і зв'язаний з ним панічний ефект для проведення фішингових кампаній, видаючи себе за оповіщення, що зв'язані з COVID-19.

Компанія Check Point, виявила, що коронавірус став інструментом хакерських атак на користувачів і бізнес. За даними експертів, з січня 2020 року в світі зареєстровано більше 4000 доменів, пов'язаних з COVID-19 [19, 20]. Серед цих сайтів знаходяться також підроблені сайти, що пропонують інформацію про COVID-19, масках або домашніх діагностичних наборах. Насправді, ці фішингові сайти використовуються хакерами для вимагання грошей або крадіжки конфіденційної, але також комерційної інформації.

За останні місяці на таких сайтах виявлені зразки програм, на яких розміщені шкідливі вкладення, установники VPN, підроблені оновлення програмного забезпечення і шкідливі мобільні додатки. Серед прикладів, з якими зазвичай стикаються фахівці, визначаються додатки, що пропонують стежити за еволюцією зараження поруч з вами, але які фактично шифрують мобільні дані, вимагаючи викуп за розблокування телефону. Загроза може ховатися в підроблених новинних сайтах, що поширюють шкідливе програмне забезпечення. Вони починають працювати, розповсюджуючи «банківський троян Grandoreiro», як тільки користувач запускає відео. Це також можуть бути електронні листи, зазвичай з вкладеннями, в яких стверджується, що вони надають інформацію про епідемію, оновлення безпеки або в привабливих пропозиціях про дефіцитну продукцію: маски або дезінфікуючі засоби. У середовищі, де люди бояться і завжди шукають додаткову інформацію, великий ризик бути спійманим за допомогою такого роду електронних листів, якщо не враховувати найкращі методи забезпечення безпеки. Тут слід віднести до

основних атак, що збільшують загрозу та забезпечують створення «зараження», наступні. Вони наведені по пунктах нижче.

1. Фішинг і копіювання фішингу: кіберзлочинці використовують ключові слова, пов'язані з COVID-19, такі як «Covid» або «Corona» в URL, для створення фішингу. Хакери просять жертв ввести свої дані для входу на підроблені сторінки входу (наприклад, Microsoft Outlook), а потім вже перенаправляють користувачів на справжні сайти. У багатьох кампаніях атаки також використовуються за допомогою макросів VBA, документів Office в якості вкладень.

2. Фальшиві сайти і фальшиві мобільні додатки: хакери впроваджують шкідливі програми Android для крадіжки даних або вимагають викуп, такий як фальшиві карти розташування випадків зараження COVID-19.

3. Відмова в обслуговуванні і цільові сторінки атаки типу «відмова в обслуговуванні» (DoS і DDoS-атаки) і перенаправлення інформації на цільові сайти, що пропонують статистичні дані про коронавірус, спотворюють доступні дані або надають явно неправдиву інформацію.

4. Підроблені VPN: програмне забезпечення підробленого VPN пропонується для завантаження співробітникам, які здійснюють дистанційну роботу.

Виникає питання про заходи, які необхідно вжити, щоб захистити саме організацію. [21, 22] У цій ситуації перша дія, яку необхідно зробити - це регулярно інструктувати співробітників про основні правила кібербезпеки і захисту від фішингових ризиків і виявити уразливості інформаційних систем і бізнес-додатків, щоб якомога швидше виправити їх і визначити пріоритети для дій в короткостроковій і середньостроковій перспективі, в залежності від бюджету.

З урахуванням наведених результатів і досвіду авторів цієї статті пропонуються наступні положення щодо забезпечення безпеки муніципальних підприємств. Вони, на наш погляд, мають розглядатися в першу чергу.

1. ***Забезпечення безпеки телероботи.***

Зростаючий трафік, перевантажені мережі і робота в небезпечних середовищах вимагають спеціальних заходів для забезпечення безпеки інформаційних потоків. Щоб справитися з цією безпрецедентною ситуацією, пропонується:

- підвищити обізнаність співробітників про ризики, пов'язані з віддаленою роботою;
- забезпечити співробітників безпечними портативними робочими станціями;
- коли неможливо розгорнути портативні робочі станції, слід розглянути можливість віддаленого доступу до закритих областям інформаційної системи через захищене з'єднання (віртуальний офіс);
- захищати архітектуру і компоненти інфраструктури віддаленого доступу (VPN);
- перевірити правильність вибору розмірів каналів зв'язку і управління якістю обслуговування потоків;
- оцінити методи безпеки і пристрої для підтримки переміщення співробітників.

2. ***Захист критично важливої інфраструктури.***

Можливі атаки, які ми спостерігаємо зараз, можуть призвести до крадіжки інтелектуальної власності, конфіденційних даних або збоїв критично важливої інфраструктури. Важливо зробити інфраструктуру стійкою до кібератак. Дані повинні регулярно захищатися і зберігатися в місцях, доступних віддалено, для відновлення в прийнятні терміни і в безпечних умовах. Інфраструктури безпеки (мережі, системи управління доступом та ідентифікацією, додатки, рішення для виявлення вторгнень або захисту) повинні бути надійними і надлишковими для забезпечення зв'язку та дотримання вимог законодавства. Коли загроза або ризик ідентифіковані, повинні бути застосовані відповідні заходи контролю, щоб дозволити підприємству видалити, обмежити, відкликати доступ і вжити відповідних заходів. Команди управління повинні гарантувати, що вони можуть виявляти і відстежувати ненормальні дії, які можуть виходити від їх співробітників, постачальників або хакерів.

3. ***Забезпечення стійкості ланцюжка роботи постачальників та надання послуг.***

Ланцюжок поставок і надання послуг можуть бути погіршені або навіть розірвані через кібератаки, націлені на постачальників або підрозділів, які надають ці послуги. Засоби, що введені в дію для кризового управління, повинні бути посилені і випробувані, а також необхідно забезпечити ефективний нагляд за критично значимими постачальниками і послугами. Тому важливо проаналізувати вплив ланцюжків додатків і технічної інфраструктури, щоб переконатися, що пристрої резервного копіювання та відновлення, що охоплюють репозиторії і бази даних, працюють, а ланцюжок посилань додатків і базові інфраструктури не пошкоджено. А саме: всі вони були захищені від вразливостей, про які повідомляють творці, або від того, що існують технічні контрзаходи, які зменшують вплив; всі були перевірені з точки зору безпеки (існування гарантованого терміну); схильні до періодичних "сканування", що забезпечує добре покриття безпеки; не мають нестачі проектування або обходу важливих баз (постачальників, послуг і т. д.); не є

предметами вразливостей, опублікованих на антихакерських сайтах вільного доступу типу DarkWeb; потенційні шляхи атаки заблоковані; основні треті сторони (субпідрядники) захищені; а поверхню атаки / вплив було зменшено.

4. ***Виявлення та блокування крадіжок або витоку даних.***

Крадіжка інформації або розкриття бази даних є більш значними ризиками в кризовий період і можуть бути викликані відсутністю обслуговування та співробітників, або відсутністю шифрування через використання невідповідних алгоритмів. Тому важливо швидко ідентифікувати характерні ознаки потерпілого в результаті атаки підприємства (і його відомі ідентифікаційні дані) в Інтернеті:

- визначити інформацію, яку зловмисник або конкурент може отримати з відкритих джерел даних;

- визначити поточні та майбутні загрози ззовні.

5***. Аналіз впливу і блокування нових атак пов'язаних з COVID-19 і шкідливих програм.***

Передбачення важливо під час кризи: отримання відповідної інформації про учасників загрози і їх можливості поставити під загрозу діяльність компанії необхідно для кращого захисту критичних систем. Цей процес може бути реалізовано за допомогою спеціальної команди CERT Ukraine або іншими фахівцями в цієї галузі за допомогою спеціалістів сервісів Cyber Threat Intelligence, які аналізують такі джерела: пошукові системи; Інтернет-сайти (блог, особистий сайт, прес-сайт і т. д.); соціальні мережі (Twitter, Facebook, Linkedin, і ін.); великі платформи для обміну файлами (dropbox і т. д.); конкретні новинні групи; IRC-канали, використовувані невеликими групами і активістами; публічну інформацію доступну на веб-сайті компанії; загальнодоступні технічні джерела (LIR, BGP, домени і т. д.); більш конфіденційні джерела інформації.

6. ***Посилення дій Центрів операцій безпеки (ЦОБ) і реагування на інциденти***.

Команди, що працюють в ЦОБ, можуть бути скорочені під час пандемії. Потім можна використовувати зовнішні ЦОБ для реагування на нові інциденти та в цих умовах працювати з інфраструктурами, в яких мають місце можливі ненадійні процеси, методами, програмним і апаратним забезпеченням.

Основні заходи у цьому напрямку, які необхідно прийняти, на наш погляд, повинні бути наступними:

- забезпечення правильної діагностики, щоб зрозуміти ступінь атаки (невелика частина муніципальних підприємств, всі муніципальні підприємства, і т. д.);

- чітке та ефективне керування комунікацією з керівництвом, як всередині, так і зовні;

- координування втручання реагування на інциденти в ситуації стресу і часто на віддалі, тобто дистанційне втручання;

- дотримання порядку управління в умовах кризи, в період її існування: виконувати вказівки кібер-експертів кризової виробничої дільниці, надавати їм поточну допомогу, зберігати докази;

- накопичення досвід, щоб прискорити прогрес у галузі, а у разі сумнівів звертатися до фахівця з інформаційної безпеки.

Висновки

При віддаленій роботі у період пандемії обов'язково збільшується доступ до мережі. Відомо, що деякі муніципальні установи є краще підготовленими до цих умов роботи. Вони мають фахівців з інформаційної безпеки, обладнання, необхідне для підтримки цілісності систем (наприклад, складних віртуальних приватних мереж (VPN), багатофакторної аутентифікації) та інші значні ресурси для виконання пропонованих вище положень, щодо забезпечення інформаційної безпеки муніципальних підприємств. Але таких установ небагато. Для більшості менш підготовлених організацій ситуація являє собою серйозну проблему. Ризик доступу співробітників до конфіденційних даних і систем через незахищені мережі або пристрої набагато вище, коли вони працюють віддалено, не кажучи вже про те, що персональні комп'ютери співробітників можуть бути більш легкою ціллю для хакерів. Тому також наполегливо рекомендується посилити моніторинг активності користувачів, що працюють вдома. Крім того, важливо інформувати співробітників про методи управління ризиками кібербезпеки, оскільки вони повинні працювати з пристроєм поза захищеної мережі організації.

Безперечним постулатом залишається те, що треба дотримуватися порядку в IT-управлінні в умовах кризи: виконувати вказівки кібер-експертів кризисної виробничої ділянки, надавати їм поточну допомогу, зберігати докази; накопичувати досвід, щоб прискорити прогрес у роботі. В разі сумнівів звертатися до фахівця з інформаційної безпеки. Нарешті, VPN необхідно регулярно оновлювати. Щоб уникнути вразливостей, мережі повинні бути протестовані, для впевненості управлінням збільшеним трафіком.

Телеробота у період пандемії може утруднити IT-персоналу моніторинг кібер-ризиків, оскільки багато цих ризиків виходять за рамки фінансових або технічних можливостей муніципальних організацій. Тому вони повинні застосовувати комплексний підхід до ризику, включаючи плани

дій в надзвичайних ситуаціях, націлений на кібер-ризики, які вказаних вище. Також можна захиститися від підвищених кібер-ризиків за допомогою страхування, яке в разі цифрового збою систем може покрити збитки, пов'язані з перебоями в роботі, а також витрати, пов'язані з наймом експертів для розслідування і усунення порушень. Дуже важливо зберігати пильність перед кіберзагрозами в розпал кризи, щоб забезпечити постійне обслуговування громадян, а також безпеку і захист їх інформації.

Література

1. Карлова, О. А. Конспект лекцій з дисципліни «Менеджмент організацій і підприємств міського господарства» (для студентів усіх форм навчання спеціальності 073 – Менеджмент) [Текст] / О. А. Карлова; Х.І. Калашнікова; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2017. – 79 с.

2. Индеева, В.В. К вопросу об определении понятия "риск". Сб. заочних электронных конференций. Электрон. дан. [Електронний ресурс] / В.В. Индеева – М.: 2009. / Российская Академия Естествознания. – Режим доступу: https://www.rae.ru/arj/2007/02/Indeeva/pdf

3. Василенко, М.Д. Право в теорії ризиків: генеза ризиків від правової до інформаційної складових (інституційний підхід) [Текст] / М.Д. Василенко, О.Б. Козін // Юридичний вісник. – О. : ВД «Гельветика». – 2019. – № 4 – С. 43-51.

4. Філософський енциклопедичний словник [Текст] / В. І. Шинкарук (гол. редкол.) та ін. – Київ : Інститут філософії імені Григорія Сковороди НАН України : Абрис, 2002. – 742 с.

5. Карлова, О.А. Менеджмент міського господарства. [Текст] Навч. посібник./ О.А. Карлова – Х.:ХНАМГ, 2008.– 266 с.

6. Шерифов, А.М. Риск-менеджмент в сфере ЖКХ: региональный аспект на примере республики [Текст] / А.М. Шерифов // Вестник Дагестанского государственного технического университета. Технические науки. №1(36). – 2015. – С. 136-142.

7. Великанова, М. М. Управління ризиком та його стадії: економіко-правовий аналіз [Текст] / М. М. Великанова // Підприємництво, господарство і право. – 2017. – № 12. – С. 20-24.

8. Мохор, В. В. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури [Текст] // В.В. Мохор, С.Ф. Гончар, О.М. Дибач // Ядерна та радіаційна безпека. – 2019. – № 2(82). – С. 4-8.

9. Cybersecurity Ventures: кибератаки происходят каждые 14 секунд [Електронний ресурс] / Компания "Ай Ти Про". – Режим доступу: https://itpro.ua/post/cybersecurity_ventures_kiberataki_proiskhodyat_kazhdye_14_sekund

10. Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. (n.d.) Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

11. 2019 Internet Crime Report Federal Bureau of Investigation. Internet Crime Complaint Center (IC3). (n.d.) Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf

12 Island hopping: правило «хорошего тона» среди кибер-преступников [Електронний ресурс] / Panda Security, 2018.– Режим доступу: https://www.cloudav.ru/mediacenter/news/island-hopping-texas-ransomware/

13. Hacked Texas government agencies face $2.5 million ransom. (n.d.) Retrieved from https://www.itpro.co.uk/security/34231/hacked-texas-government-agencies-face-25-million-ransom

14. Хакеры взяли в заложники Балтимор: 10 тысяч административных компьютеров до сих пор блокированы [Електронний ресурс] / Сетевое издание «Агентство кибербезопасности». – Режим доступу: https://bezmaly.wordpress.com/2019/06/07/robbinhood/

15. Хакеры вывели из строя компьютерные системы госучреждений Балтимора с помощью разработки АНБ, использовавшейся в атаках WannaCry и NotPetya в 2017 году [Електронний ресурс] / ООО «ХОТЛАЙН» – Режим доступу: https://itc.ua/news/hakery-vyveli-iz-stroya-kompyuternye-sistemy-gosuchrezhdenij-baltimora-s-pomoshhyu-razrabotki-anb-ispolzovavshejsya-v-atakah-wannacry-i-notpetya-v-2017-godu/

16. Hackers Are Holding Baltimore Hostage: How They Struck and What's Next. (n.d.) Retrieved from https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

17. Власти американского города заплатили хакерам $500 000 в биткоинах [Електронний ресурс] / "Компьютерра" 1997-2020. – Режим доступу: https://www.computerra.ru/238941/vlasti-amerikanskogo-goroda-zaplatili-hakeram-500-000-v-bitkoinah/

18. Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts. (n.d.) Retrieved from https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html

19. Check Point: зарегистрировано более 4000 доменов, связанных с COVID-19 [Електронний ресурс] / Сетевое издание – Хакер. – Режим доступу: https://xakep.ru/2020/03/10/covid-19/

20. Update: Coronavirus-themed domains 50% more likely to be malicious than other domains. (n.d.) Retrieved from https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

21. COVID-19 : cinq mesures pour se défendre contre les cyberattaques [Електронний ресурс] / Компанія "Ernst & Young Global Limited". Режим доступу: https://www.ey.com/fr/fr/services/advisory/covid-19-les-mesures-a-prendre-pour-renforcer-votre-cybersecurite

22. Barnet Sherman (2020) Municipal Cybersecurity: Governance Metrics For ESG Investors [Електронний ресурс] / Forbes Media. – Режим доступу:

https://www.forbes.com/sites/investor/2020/02/04/municipal-cybersecurity--governance-metrics-for-esg-investors/#514b4de15a60

References

1. Karlova, O. A., & Kalashnikova, Kh. I. (2017) Konspekt lektsii z dystsypliny «Menedzhment orhanizatsii i pidpryiemstv miskoho hospodarstva» (dlia studentiv usikh form navchannia spetsialnosti 073 – Menedzhment) [Lecture notes on the subject "Management of organizations and enterprises of municipal economy" (for students of all forms of education specialty 073 - Management]. Kharkiv. nats. un-t misk. hosp-va im. O. M. Beketova. – Kharkiv : KhNUMH im. O. M. Beketova, 2017. – 79 . [in Ukrainian].

2. Indeeva, V.V. (2009) K voprosu ob opredelenyy poniatyia “rysk” [On the question of defining the concept of "risk"]. Materials of correspondence electronic conferences. Russian Academy of Natural Sciences. Retrieved from: https://www.rae.ru/arj/2007/02/Indeeva/pdf [In Russian].

3. Vasilenko, M.D., & Kozin, O.B. (2019) Law in risk theory: genesis of risks from legal to information components (institutional approach). *Legal Bulletin. "Helvetica". 4,* 43-51 [in Ukrainian].

4. Shinkaruk, V. I. (Eds.). (2008) Filosofskyi entsyklopedychnyi slovnyk [Philosophical encyclopedic dictionary]. Kyiv : Instytut filosofii imeni Hryhoriia Skovorody NAN Ukrainy [in Ukrainian].

5. Karlova, O.A. (2008) Menedzhment miskogo gospodarstva. [Municipal management]. Navch. posIbnik. – H.: HNAMG [in Ukrainian].

6. Sherifov, A.M. (2015) Risk-menedzhment v sfere ZhKH: regionalnyiy aspekt na primere respubliki Dagestan. [Risk management in the field of housing and communal services: a regional aspect on the example of the Republic of Dagestan]. Vestnik Dagestanskogo gosudarstvennogo tehnicheskogo universiteta. Tehnicheskie nauki [*Bulletin of Dagestan State Technical University. Technical sciences]*. *1 (36).* 136-142 [In Russian].

7. Velikanova, M.M. (2017) Upravlinnya rizikom ta yogo stadiyi: ekonomIko-pravoviy analiz [Risk management and its stages: economic and legal analysis]. Pidprie mnitstvo, gospodarstvo i pravo [*Entrepreneurship, economy and law]*. *12*, 20-24 [in Ukrainian].

8. Mokhor, V.V., Gonchar, S.F., & Dybach, O.M. (2019) Metodi otsinki sumarnogo riziku kiberbezpeki ob’ektiv kritichnoyi infrastrukturi [Methods for assessing the total risk of cybersecurity of critical infrastructure] Yaderna ta radiatsiyna bezpeka *[Nuclear and radiation safety]*. *2(82)*, 4-8 [in Ukrainian].

9. “IT Pro” Company (2020) Cybersecurity Ventures: Cybersecurity Ventures: kiberataki proishodyat kazhdyie 14 sekund [cyberattacks occur every 14 seconds]. Retrieved from: https://itpro.ua/post/cybersecurity_ventures_kiberataki_proiskhodyat_kazhdye_14_sekund

10. Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. (n.d.) Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

11. 2019 Internet Crime Report Federal Bureau of Investigation. Internet Crime Complaint Center (IC3). (n.d.) Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf

12. Panda Security (2020) Island hopping: pravilo «horoshego tona» sredi kiber-prestupnikov [Island hopping: the rule of "good manners" among cybercriminals]. Retrieved from: https://www.cloudav.ru/mediacenter/news/island-hopping-texas-ransomware. [In Russian].

13. Hacked Texas government agencies face $2.5 million ransom. (n.d.) Retrieved from https://www.itpro.co.uk/security/34231/hacked-texas-government-agencies-face-25-million-ransom

14. Bezmaly, V.(2019) Hakeryi vzyali v zalozhniki Baltimor: 10 tyisyach administrativnyih kompyuterov do sih por blokirovanyi. [Hackers took Baltimore hostage: 10 thousand administrative computers are still blocked]. Retrieved from: https://bezmaly.wordpress.com/2019/06/07/robbinhood. [In Russian].

15. Skripin, V. (2019) Hakeryi vyiveli iz stroya kompyuternyie sistemyi gosuchrezhdeniy Baltimora s pomoschyu razrabotki ANB, ispolzovavsheysya v atakah WannaCry i NotPetya v 2017 godu [Hackers disabled the computer systems of Baltimore government agencies through the development of the NSA, used in the attacks of WannaCry and NotPetya in 2017]. Retrieved from: https://itc.ua/news/hakery-vyveli -iz-stroya-kompyuternye-sistemy-gosuchrezhdenij-baltimora-s-pomoshhyu-razrabotki-anb-ispolzovavshejsya-v-atakah-wannacry-i-notpetya-v-2017-godu / [In Russian].

16. Hackers Are Holding Baltimore Hostage: How They Struck and What’s Next. (n.d.) Retrieved from https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

17. Makina, S. (2019) American city authorities paid hackers $ 500,000 in bitcoins. Retrieved from: https://www.computerra.ru/238941/vlasti-amerikanskogo-goroda-zaplatili-hakeram-500-000-v-bitkoinah/ [In Russian].

18. Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts. (n.d.) Retrieved from https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html

19. Nefyodova, M. (2020) Check Point: zaregistrirovano bolee 4000 domenov, svyazannyih s COVID-19 [Check Point: registered more than 4000 domains related to COVID-19]. Retrieved from: https://xakep.ru/2020/03/10/covid-19/ [In Russian].

20. Update: Coronavirus-themed domains 50% more likely to be malicious than other domains. (n.d.) Retrieved from https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

21. "Ernst & Young Global Limited" (2020) COVID-19 : cinq mesures pour se défendre contre les cyberattaques. Retrieved from: https://www.ey.com/fr/fr/services/advisory/covid-19-les-mesures-a-prendre-pour-renforcer-votre-cybersecurite
22. Barnet Sherman (2020) Municipal Cybersecurity: Governance Metrics For ESG Investors. Retrieved from: https://www.forbes.com/sites/investor/2020/02/04/municipal-cybersecurity--governance-metrics-for-esg-investors/#514b4de15a60

Рецензент: доктор технічних наук, професор, завідувач кафедри В.М. Тупкало, Київський інститут інтелектуальної власності та права Національного Університету "Одеська юридична академія", Київ, Україна

Автор: ВАСИЛЕНКО Микола Дмитрович
доктор фізико-математичних наук, доктор юридичних наук, професор, завідувач кафедри кібербезпеки
Національний університет «Одеська юридична академія»
E-mail – nvas08@ukr.net
ID ORCID: http://orcid.org/0000-0002-8555-5712

Автор: КОЗІН Олександр Борисович
кандидат фізико-математичних наук, доцент, доцент кафедри
Національний університет «Одеська юридична академія»
E-mail – alexnazaret1@gmail.com
ID ORCID: http://orcid.org/0000-0001-8071-4000

Автор: КОЗІНА Марія Олександрівна
кандидат технічних наук, доцент, старший викладач кафедри
Національний університет «Одеська юридична академія»
E-mail – mashak_od@ukr.net
ID ORCID: http://orcid.org/0000-0001-8967-7218

Автор: РАЧУК Валерій Олександрович
асистент кафедри
Національний університет «Одеська юридична академія»
E-mail – rachuk960@gmail.com
ID ORCID: http://orcid.org/ 0000-0003-1793-016X

CYBER RISKS IN THE MUNICIPAL ECONOMY DURING THE PANDEMIC: DAMAGES AND THE STRUGGLE FOR CYBER SECURITY

M. Vasilenko, O. Kozin, M. Kozina, V. Rachuk
National University "Odessa Law Academy", Ukraine

As a result of remote control and automation, the urban infrastructure becomes extremely vulnerable to intrusions, attacks, human errors, accidents that are growing. Due to the concentration of local and global computer networks, systems and software, the "cyber risk" of the municipal economy is multiplicative, which makes it systemic and international. Its essence is manifested both at the national and global levels through the impact on business, municipal and state authorities. Today, the existing pandemic contributes to an increase in the number of cyberattacks, which indicates an even greater cyber vulnerability of municipal administrations and public authorities. Coronavirus COVID-19 has become a tool for hacker attacks on users and enterprises. The purpose of the article is to determine, based on a systematic analysis of the new cyber risks of the municipal economy that arose during the pandemic, to formulate our own views on the classification and methods of counteracting municipal organizations and enterprises. According to experts, since the beginning of this year, thousands of domains associated with coronavirus have been registered in the world. This number also includes sites of various hacker groups that offer information about coronavirus, masks, or quick treatment methods. In fact, these phishing sites are used by hackers to extort money or steal confidential, as well as commercial information. The main types of attacks that increase the threat and actually create a "cyber infection" are noted. Based on the material of this article and the experience of the authors, measures are proposed that ensure the safety of municipal enterprises, which should be carried out in the first place. Strict measures in IT management during a crisis are also recognized as undeniable and necessary. Such as help from cyber experts and help for cyber experts; preservation of evidence of intrusion, staff training, accumulation of experience to accelerate progress in work. Remote work during a pandemic can make it difficult for IT staff to monitor cyber risks, since many of these risks go beyond the financial or technical capabilities of municipalities. Therefore, based on these proposals for the safety of municipal enterprises, an integrated approach to cyber risks is proposed, including an emergency response plan. Based on international experience, the possibility of insuring municipal enterprises and organizations against potential losses associated with cyber attacks by hackers, as well as to eliminate the consequences of these attacks, is also noted.

Keywords: *cyber-security, cyber-risk, municipal economy, "phishing", pandemic, Covid-19*