продукцією; уміння формувати та зберігати стандартні і регламентовані звіти дозволить в майбутньому працювати в різних програмних продуктах.

Успішне проходження навчальної практики дає можливість брати участь та мати високі досягнення у Міжнародній студентській Олімпіаді в сфері інформаційних технологій «IT-Universe» конкурс «Використання автоматизованих систем обліку та підвищує конкурентоздатність випускників коледжу на ринку праці. Під час проходження виробничої практики окремі студенти надавали допомогу фермерським господарствам у впровадженні бухгалтерської програми конфігурація «Бухгалтерія сільськогосподарського підприємства».

Полторак А.С.
доктор економічних наук, доцент,
доцент кафедри фінансів, банківської справи та страхування
Миколаївський національний агарний університет
Жовта Н.А.
здобувач вищої освіти обліково-фінансового факультету
Миколаївський національний аграрний університет

КІБЕРГІГІЄНА У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ

Кожного дня інформаційні технології все стають невіддільною частиною життя сучасної людини. Сьогодні більшість громадян має смартфон з доступом до Інтернет-мережі, що дозволяє завжди бути онлайн. У будь-який момент існує можливість перевірити пошту чи месенджер, купити квиток в кіно чи забронювати житло для відпустки, здійснювати платежі, не звертаючись до відділень банку. Всі ці дії в Інтернеті передбачають обмін певною особистою інформацією чи конфіденційними даними, які у разі неуважності або

недостатнього рівня цифрової грамотності можуть опинитися в руках зловмисників.

Кількість інтернет-шахрайств, фактів втручання в особистий інформаційний простір, поширення неправдивих відомостей нині набуває рис епідемії, особливо у сфері фінансів та банкінгу. Отже, поняття «кібергігієна» є актуальною темою сьогодення, що може забезпечити кращий захист користувача від кібератак і витоків даних.

Для забезпечення захисту персональних даних під час роботи в Інтернет-мережі спеціалісти ESET рекомендують дотримуватися основних правил кібергігієни. Своєю чергою, кібергігієна – це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації [1]. Сьогодні досить розповсюдженими є кібератаки на сервіси банкінгу та клієнтські бази з повними даними про особу. Саме тому дотримання елементарних правил кібергігієни є обов'язковим.

До основних правил кібергігієни для покращення захисту даних належать:

1. Перевірка безпеки активних акаунтів (облікових записів електронної пошти та акаунтів в соцмережах). Існують веб-сайти, що допоможуть з'ясувати, чи був пароль до електронної пошти викрадений зловмисниками.

2. Аналіз програм. Це правило полягає у ґрунтовному аналізі вже завантажених додатків, видаленні непотрібних та контролі встановлення кожної програми. Також під час завантаження додатку варто звертати увагу на дозволи, які ви надаєте.

3. Регулярне оновлення. Для запобігання інфікуванню шкідливими програмами варто здійснювати своєчасне оновлення операційної системи та окремих додатків, яке передбачає виправлення вразливостей та помилок в програмному забезпеченні.

4. Надійний пароль, встановлений з метою запобігання несанкціонованому доступу до пристроїв. Важливо переконатися у надійності ваших паролів завдяки створенню складної комбінації, яка містить не менше 12 символів, великі та малі літери, цифри та символи. Крім цього, для кожного акаунта варто використовувати унікальний пароль.

5. Додатковий рівень захисту. Для покращення безпеки облікових записів доцільно застосовувати двофакторну аутентифікацію, яка передбачає підтвердження особистості під час входу в певний акаунт.

6. Регулярне резервне копіювання, яке сприятиме відновленню потрібних даних у разі їх шифрування програмою-вимагачем або видалення шкідливим програмним забезпеченням.

7. Надійний захист від різних загроз, зокрема програм-вимагачів, шпигунських програм, вірусів, троянів та фішинг-атак [1].

Дотримання цих правил, на нашу думку, ускладнює процес використання гаджетів, але профіт від дотримання кібергігієни з легкістю нівелює будь-який дискомфорт.

Користувачі характеризуються важливою роллю в забезпеченні безпеки цифрового суспільства, підвищуючи його інформованість і практикуючи забезпечення «кібергігієни». Кваліфіковані фахівці і підприємства в області кібербезпеки повинні співпрацювати, підвищувати обізнаність користувачів про кібербезпеку.

Краща стратегія захисту – знати заздалегідь, звідки саме чекати загрози, та який алгоритм дій необхідно застосувати для уникнення зустрічі з нею. Так, досвідчений користувач ніколи не видасть свій пароль зловмиснику, тому що знає, що легітимні працівники банківських установ ніколи не здійснюють подібних запитів.

Сьогодні саме уряд формує стратегію кібербезпеки в цілому, визначає рівень об’єктів критичної інфраструктури та державних корпорацій, які передусім потребують захисту, а

також рівень приватних компаній та груп, що мають відчувати підтримку держави та водночас дотримуватись правилами та нормами інформаційної безпеки, наявними у законодавстві.

Така схема організації розгалуженого захисту країни є достатньо ефективною та дозволяє: розподілити пріоритети захисту, виявити та нейтралізувати потенційні уразливості у інфраструктурі вищого рівня, розподілити повноваження: який орган і що має захищати, формувати законодавчо-нормативну базу, здатну відповідати сучасним умовам.

В Україні намагаються підвищити ступінь цифрової грамотності за допомогою освітньої платформи Міністерства цифрової трансформації України Дія.Цифрова Освіта. На даній платформі розміщено освітній серіал про правила кібергігієни для державних службовців, який складається з 9 серій тривалістю 3-7 хвилин. Створено даний серіал за підтримки Координатора проєктів ОБСЄ в Україні та було представлено 26 січня 2021 року на заході в Києві.

Генрік Вілладсен, Координатор проєктів ОБСЄ в Україні зазначив: «Сучасне урядування неможливе без інформаційних технологій, але ці технології створюють нові ризики, оскільки злочинці або терористи прагнуть знайти та використати вразливості цифрових технологій, щоб пошкодити чи порушити роботу державних інформаційних систем. Масштаб можливого збитку від злочинів, скоєних за допомогою інформаційних технологій, надзвичайно зріс за останні роки. Інформувати посадовців про ці ризики та про те, що вони можуть і повинні зробити для підвищення цифрової безпеки своїх установ, є ключовим кроком у формуванні стійкості країни до сучасних загроз» [2].

Дані освітні матеріали сприятимуть підвищенню рівня цифрової грамотності стосовно: правил кібергігієни на роботі й у повсякденні; безпечного користування браузером та загалом мережами Wi-Fi; розмежовування використання особистої та службової поштових скриньок; використання програмного забезпечення; відповідального поширення інформації у

соціальних мережах; правил безпечної роботи з мобільними пристроями; видів маніпуляцій з інформацією у кіберсфері і т.д. [3].

Отже, кібергігієна як спосіб захисту має вищу ієрархію та більшу цінність, ніж різноманітне антивірусне програмне забезпечення. Ефективнішим рішенням є недопущення зараження власного пристрою шляхом дотримання простих правил безпеки (відмова від завантаження невідомих файлів без підпису та видавця, ігнорування фішингових сторінок і т.д.), ніж боротьба з наслідками цього зараження, покладаючись на потужність антивірусного програмного забезпечення.

Перелік використаної літератури:

1. Основні правила захисту даних – кібергігієна для активного Інтернет-користувача. URL: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya# (дата звернення: 01.02.2021).

2. Освітній серіал, створений за підтримки ОБСЄ, популяризуватиме кібергігієну серед держслужбовців України. URL: https://www.osce.org/uk/project-coordinator-in-ukraine/476542 (дата звернення: 01.02.2021).

3. Освітня платформа Міністерства цифрової трансформації України Дія.Цифрова Освіта. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene (дата звернення: 01.02.2021).

4. Полторак А.С. Фінансова безпека держави в умовах глобалізації: теорія, методологія та практика : монографія. Миколаїв : МНАУ, 2019. 463 с. URL: https://cutt.ly/BgrWXXx (дата звернення: 01.02.2021).

5. Полторак А.С., Баришевська І.В., Мельник О.І., Боднар О.А. Кібернетична безпека банківського сектора в системі фінансової безпеки держави. *Сучасні тенденції розвитку фінансово-кредитної системи: теорія та практика* :

колективна монографія; Київ : Центр фінансово-економічних наукових досліджень, 2019. С. 79-83.

Попіль О.М.
спеціаліст другої категорії
Відокремлений структурний підрозділ «Заліщицький фаховий коледж імені Є.Храпливого НУБіП України»

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НАВЧАННЯ У ПІДГОТОВЦІ ФАХІВЦІВ В УМОВАХ СУЧАСНОСТІ

Якість життя і освітній потенціал українського суспільства багато в чому визначається рівнем освіти і культури населення, його світоглядною орієнтацією і духовним розвитком, можливістю систематично отримувати і використовувати необхідну інформацію. Ці чинники впливають на ступінь включенності українського суспільства в національні і світові загальнолюдські процеси прогресивного розвитку. Освіта, що відповідає сучасним потребам суспільства і ринку праці, виступає могутнім адаптивним потенціалом у швидкоплинному трансформуючому суспільстві до сучасних соціоекономічних реалій, що стає найважливішою умовою успішного і стійкого суспільного розвитку [1].

В умовах сьогодення людина розглядається як суб'єкт, який активно і свідомо використовує інформаційні технології для здобуття знань і навичок. На думку Дубасенюк О. А. система освіти створюється для людини, функціонує і розвивається в її інтересах, слугує повноцінному розвитку творчої особистості. За дослідженнями Дичківської І.М освіта за своїм змістом, формами і методами є змінною, оскільки вона має реагувати на нові цивілізаційні виклики, суспільні реалії, враховуючи тенденції, перспективи розвитку людства, національного буття народу.

Термін "інновація" (із пізньолатинської innoyatio -