

**Мозгаллі О.П., д.е.н.,**  
професор кафедри інформаційних систем в економіці  
**Рибалко Я.В.,**  
аспірант кафедри інформаційних систем в економіці  
**Синицький Р.К.,**  
магістр спеціалізації «Інформаційні управляючі системи та технології»  
Київський національний економічний університет імені Вадима Гетьмана

**Mozgalli O.P.,** Doctor of Economic Science,  
Professor of the Economics Information Systems Department,  
**Rybalko Y.V.,** Postgraduate of the Economics  
Information Systems Department,  
**Synytskyi R.K.,** Master Student at the  
«Information management systems and technology» speciality,  
Kyiv National Economic University named after Vadym Hetman

## ІНФОРМАЦІЙНА БЕЗПЕКА У ЦИФРОВІЙ ОСВІТІ В УКРАЇНІ

### INFORMATION SECURITY OF DIGITAL EDUCATION IN UKRAINE

**Анотація.** У статті висвітлено терміни та основні аспекти пов'язані з цифровізацією освіти, кібербезпекою та персональними даними. Взнявши за мету дослідити аспекти інформаційної безпеки у цифровій освіті в межах України, спираючись на Європейський досвід, проаналізовано матеріали та дослідження, серед яких було вказано, що в своєму дослідженні В.Я. Певнев від 2010 року каже про те, що інформаційної безпеки як такої не існує в універсальному десятковому класифікаторі. Наразі інформаційна безпека складається з багатьох факторів, як каже сам автор В.Я. Певнев, проте, якщо казати про загальноприйнятту класифікацію і розподілення підтипів інформаційної безпеки, про те, що інформаційна безпека в цілому складається з трьох головних частин, то можна зробити висновок, що сама по собі інформаційна безпека існує в десятковому класифікаторі, і так само як і в міжнародних класифікаторах, але по частинах. Якщо подивитись на реалії, то в General Data Protection Reglament можна побачити вимоги до конфіденційності, проте як вказано у статті [9], лише при роботі з підприємствами або громадянами ЄС цей регламент вступає в силу на території України. Тому на прикладі Європейського досвіду було проведено аналіз складових цифрової освіти, а саме інформаційної безпеки. І на основі матеріалів про базові існуючі атаки, захист від них і дослідження базової взаємодії користувача з Європейським GDPR, було зроблено висновок, що існує можливість зменшити втрати персональних даних користувачів, та дозволити їм контролювати свої персональні дані, якщо ввести в експлуатацію GDPR. Введення GDPR також дозволить контролювати загальне користування базами рекламних агентів, а саме персональною інформацією, що її надають звичайні користувачі у кіберпросторі. Проблемами введення та використання GDPR на теренах України є популярною та одною з ключових точок розвитку кібер-законодавства.

**Ключові слова:** цифровізація, освіта, інформаційна безпека, захист даних.

**Abstract.** *The article covers the terms and main aspects related to digitalization of education, cybersecurity and personal data. The aim was to explore aspects of information security in digital education within Ukraine, based on the European experience. Materials and studies were analyzed, among which it was stated that in his 2010 study, Pevnev said that information security as such does not exist in the universal decimal classifier. Information security now has many factors, according to Pevnev himself. If we talk about the common classification and distribution of information security subtypes, that information security as a whole consists of three main parts, we can conclude that information security itself exists in a separate form in the decimal classifier as well as in international classifiers. If you look at the realities, you can see the privacy requirements in the General Data Protection Regulation. As stated in Article [9], only when working with enterprises or citizens of the European Union this regulation does enter into force on the territory of Ukraine. Therefore, an example of the European experience has been to analyze the information security as a component of digital education. Basic existing attacks and defense against them are analyzed. User interaction with European GDPR has been researched. It is possible to reduce the loss of personal data of users and allow them to control their personal data. To reduce the loss of data GDPR can be used. The introduction of General Data Protection Regulation will also allow you to control the shared use of advertising agent databases and personal information provided by ordinary users in cyberspace. The issue of introducing and using GDPR in the territory of Ukraine is popular and one of the key points in the progress of cyber legislation.*

**Key words:** *digitalization, education, information security, data protection.*

**Вступ.** Цифровізація в Україні досить нове для країни явище у порівнянні з провідними країнами світу. Проте дивлячись на організацію цифровізації освіти за кордоном, ми можемо зробити певні висновки. Освіту явище цифровізації також не оминуло. Цифровізація освіти сприяє розвитку різноманітних сфер діяльності людини та її повсякденного життя. Найпомітніший вплив у сферах економіки, бізнесу, суспільства та життєдіяльності країни. Проте, при впровадженні цифрової освіти можна зіткнутися з багатьма проблемами, серед яких найважливішу роль для людини, що користується такою системою, відіграє інформаційна безпека. Тому наразі необхідно зосередити увагу на можливих атаках та способах захисту від них саме в сфері цифрової освіти, через її вплив на інші сфери.

**Постановка проблеми:** дослідити аспекти інформаційної безпеки у цифровій освіті в межах України, спираючись на Європейський досвід. Порівняти існуючі проблеми з інформаційною безпекою в цифровій освіті в Україні та в Європі. Також метою даної статті було виявити та проаналізувати приклади вразливостей у джерелах цифрової освіти в межах України.

**Виклад основного матеріалу.** Цифровою освітою є об'єднання різних компонентів і найсучасніших технологій завдяки використанню цифрових платформ, впровадженню нових

інформаційних та освітніх технологій, застосуванню прогресивних форм організації освітнього процесу та активних методів навчання, а також сучасних навчально-методичних матеріалів.

Основними напрямками цифровізації освіти є:

- створення освітянських ресурсів і цифрових платформ з підтримкою інтерактивного та мультимедійного контенту для загального доступу закладів освіти та учнів, зокрема інструментів автоматизації головних процесів роботи навчальних закладів;

- розроблення та впровадження інноваційних комп'ютерних, мультимедійних і комп'ютерно-орієнтованих засобів навчання та обладнання для створення цифрового навчального середовища (мультимедійні класи, науково-дослідних STEM-центрів лабораторії, інклюзивні класи, класи змішаного навчання);

- організація широкосмугового доступу до Інтернету учнів і студентів у навчальних класах та аудиторіях у закладах освіти всіх рівнів;

- розвиток дистанційної форми освіти з використанням когнітивних і мультимедійних технологій [1].

Одним із головних аспектів стабільної роботи сфери цифрової освіти є її захищеність, тож необхідно звернути увагу на інформаційну безпеку кожної людини в таких системах та інформаційну безпеку систем цифровізації освіти в цілому як критично важливих об'єктів інфраструктури.

Кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

Кіберзахист — сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

Критично важливі об'єкти інфраструктури (далі — об'єкти критичної інфраструктури) — підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити нега-

тивний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [2].

Так як система вміщує в собі персональну інформацію про фізичну особу, то захист спрямований на запобігання несанкціонованих дій з інформацією про фізичну особу.

Інформація про фізичну особу (персональні дані) — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом [3].

Несанкціоновані дії щодо інформації в системі — дії, що проводяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства [4].

Існує багато типів атак на системи цифрової освіти, що можуть не тільки пригальмувати, а й взагалі зупинити навчання. Через те, що основну частину цифрової освіти в світі займають саме веб-ресурси, то вони певна річ є найуразливішим місцем системи. Розглянемо найпоширеніші типи атак на веб-ресурси та підготовчі етапи до них, помітивши які буде можливість вчасно зреагувати та випередити зловмисника.

**Дослідження мережі.** Даний тип дій зі сторони зловмисника не передбачає ніяких руйнівних чи шкідливих дій. У більшості випадків мається на увазі лише збір даних про сервери, персональні комп'ютери та будь-які пристрої, що можуть бути підключені до тієї-ж мережі що й "жертва". Зазвичай сканування мережі проводять перед достатньо серйозною та цілеспрямованою атакою.

Сніффінг пакетів або пошук пакетів теж відноситься до дослідження мережі, адже принцип заснований на особливостях роботи мережі та персональних комп'ютерів у ній. Пакети що отримані сервером або будь-яким персональним комп'ютером у мережі пересилаються на обробку, де їх обробляє спеціальний додаток, через що зловмисник може отримати доступ не тільки до інформації про структуру самої електронно-обчислювальної

машини, але і до тієї інформації, що була безпосередньо передана, тобто паролі, повідомлення та будь-які файли.

IP-спуфінг — це підготовчий аспект до серйозної атаки, проте це також є окремим типом атаки. За допомогою IP-спуфінгу комп'ютер зловмисника може використати IP-адреси, що входять до атакованої локальної мережі. Атака також можлива, якщо система безпеки не передбачає ідентифікацію IP-адреса, та не вимагає додаткових умов.

**Атаки.** Mailbombing є найстарішим типом. Сенс атаки у тому, що трафік як і кількість повідомлень між клієнтом і сервером значно збільшується, що і призводить до збоїв, або до інших проблем у роботі серверу або клієнту. Також це викликає зупинку поштового серверу, що впливає на пересилання повідомлень між адресатами. На сьогоднішній день ефективність таких атак є нульовою, оскільки більшість провайдерів в Україні можуть встановити обмеження трафіку від одного відправника до іншого, або до серверу.

Часто, на погано захищених серверах, використовують переповнення буферу пам'яті, що є програмними помилками в кодї. При цих помилках пам'ять серверу порушує свої допустимі кордони доступу, що, в свою чергу, змушує процес завершитись аварійно, або запускає на виконання сервером довільний бінарний код, де може використовуватись поточний обліковий запис. Частіше за все обліковий запис буде адміністратору ресурсу, через що можна отримати несанкціонований доступ до ресурсу.

DDoS (Distributed Denial of Service) — підтип, що має ту ж мету, що і переповнення буферу, але ця атака відбувається не з одного комп'ютера, а з багатьох комп'ютерів в мережі. Тут як і в типї атаки “переповнення буферу” використовується спосіб використати сторонній програмний код і відмова в обслуговуванні системи за для зупинки серверу абощо. DDoS використовується там, де звичайний DoS не є ефективним. Для цього кілька комп'ютерів у мережі об'єднують, кожен з яких проводить свою DoS-атаку на систему “жертви”. Усі ці дії загалом називаються DDoS-атака.

Для більш захищених серверів використовуються віруси, трояни, поштові черв'яки та сніфери. Даний тип атак об'єднує різні негативні програмні засоби. Призначення і принципи дії таких програмних засобів буде найрізноманітнішим, адже неможливо передбачити що саме шукає дане програмне забезпечення. Кожна програма має свою мету та тип дій на сервері або персональному комп'ютері користувача. Вірус найчастіше вражає систему не

даючи їх нормально працювати. Троян найчастіше намагатиметься вкрасти будь-які дані, до яких зможе отримати доступ, так само як і поштовий черв'як, тільки останній розповсюджується електронною поштою. Проте через наявність гарних систем захисту вже не є актуальним. Сніфери призначені лише для виявлення даних всередині системи.

Якщо ж зловмисник має прямий доступ до мережі, то він може використати тип атаки “Man-in-the-middle”. Тип атаки, коли зловмисник перехоплює всі дані між двома додатками з двох різних персональних комп'ютерів, у результаті чого отримує доступ до всієї інформації, що проходить від одного користувача до іншого. Метою такої атаки є не тільки крадіжка даних або файлів, а й теоретично фальсифікація інформації для того, кому вона була призначена.

Для веб-ресурсів або до ресурсів, що мають доступ до баз даних найчастіше використовується ін'єкція. Цей тип атак доволі широкий основним принципом котрих є введення до будь-якої системи своєї частини програмного коду, що не заважає роботі системи чи програми а й виконує певні дії, що необхідні зловмиснику.

Brute force більше відомий як метод грубої сили або ж як метод повного перебору. Суть методу заключається в повному переборі всіх можливих варіантів ключу доступу, що вимагає багато часу та достатніх потужностей машини атакуючого. Найчастіше використовується для незахищених сторінок доступу до адміністраторських можливостей чи для пошуку стандартних пар логін-пароль.

І останнє по списку, але не останнє в арсеналі можливостей зловмисників — соціальна інженерія. Якщо до цього зловмисники намагались дістатись до інформації через програмні засоби та персональні комп'ютери, то мета соціальної інженерії — отримати доступ до інформації через недосконалості людини. Будь-яка риса людини може бути обернена проти неї задля здобуття інформації про цю ж людину або компанію, тощо.

Тож постає питання, яким чином можна захистити системи цифровізації освіти від зловмисників чи просто недобросовісних людей, що бажають залізти до системи та щось змінити зсередини не маючи на те прав.

Наразі існує багато різних систем захисту. Певні рішення можна використовувати як для персональних комп'ютерів, так і для серверних систем, що мають витримувати більші навантаження ніж звичайні користувацькі машини. Використовуючи кілька систем захисту в тандемі можна зменшити шанс проникнення до вашої системи майже до мінімуму.

Всі основні системи захисту можна поділити на три типи (рис. 1), фізичний, зовнішні та програмні, останні два з яких розділяються на активні та пасивні.

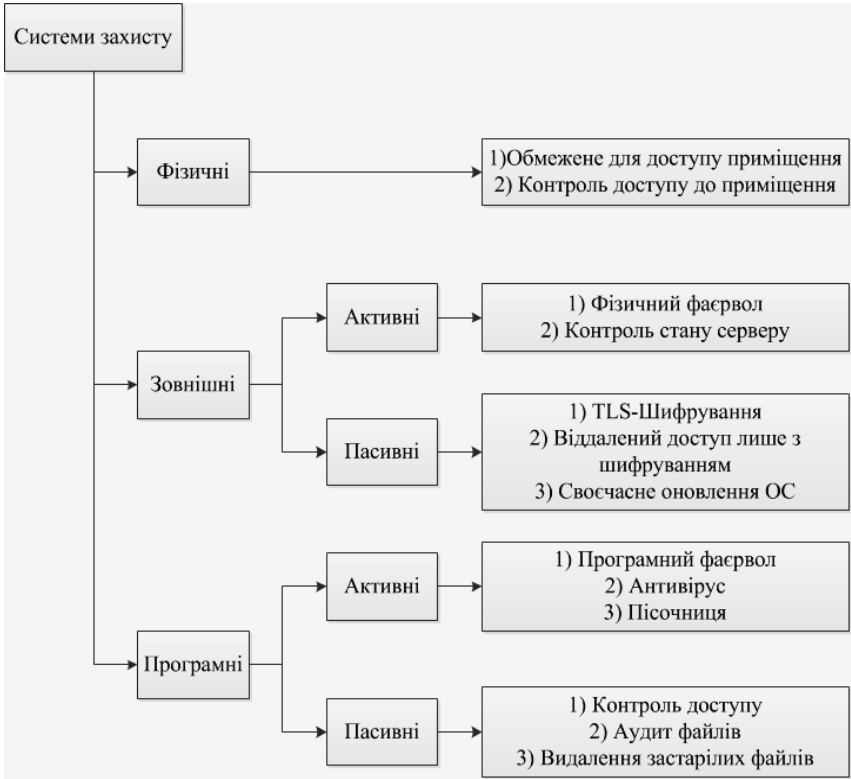


Рис. 1. Розподілення систем захисту

Фізичні системи захисту — це рішення, що дозволяють захистити сервер цифрової освіти від фізичного доступу сторонніми особами, мінімізуючи втручання в роботу системи. В той час, як закриті приміщення не є великою перешкодою, посилення контролю доступу за допомогою відеонагляду або карток доступу значно ускладнює несанкціонований фізичний доступ до приміщення.

Зовнішні системи захисту можна поділити на активні та пасивні. Зовнішні активні системи — це рішення, що дозволяють активно захищати сервер утворюючи “захисний шар” ще до серверу. До активних систем можна віднести фізичний фаєрвол. На відміну від програмного фаєрволу — фізичний фаєрвол є окре-

ним пристроєм або групою пристроїв зі своєю окремо налаштованою системою, що шифрує трафік, коригує доступ до серверу на основі певних встановлених правил. Але так само необхідно наглядати за сервером у режимі реального часу, адже будь-який неочікуваний сплеск активності може вказувати на загрозу.

До зовнішніх пасивних систем можна віднести ті, що є одно-разово налаштованими і використовуються без змін, та ті, що відносяться до обох сторін користування. TLS-шифрування необхідно використовувати задля забезпечення безперервно-надійного з'єднання користувача з сервером у веб-режимі, наприклад викладача у момент виставлення балів до системи навчання. Через можливість перехоплення трафіку, для віддаленого керування сервером, або будь-яких технічних робіт персонал має використовувати захищене з'єднання, задля забезпечення безпеки даних користувачів. Також до зовнішніх пасивних систем відносяться оновлення програмного забезпечення, так як це залежить від розробників мережевої операційної системи.

Завершальним типом систем захисту є програмні, тобто системи що працюють зсередини серверу, або персонального комп'ютеру. Їх так само, як і зовнішні системи можна поділити на активні та пасивні. До активних можна віднести програмний фаїрвол, що на відміну від апаратного працює вже всередині системи, контролюючи усі переміщення та потоки. Також сюди входить і антивірус, що необхідний за для пошуку шкідливих програмних засобів. В антивірус зазвичай входить такий інструмент, як пісочниця для програм і програмних засобів, але якщо такої пісочниці немає в антивірусі, то вона має бути окремою. Пісочниця допомагає відокремити перший запуск будь-якої програми від системи та перевірити, чи є вона шкідливою.

До пасивних внутрішніх систем захисту можна віднести певні правила та застереження, що контролюються сервером. Найпростіше обмеження доступу до певних файлів допоможе утримати систему та дані в ній в цілісності. Аудит файлів у свою чергу допоможе порівняти початковий розмір системних файлів із кінцевим після запуску системи та виявити до яких файлів намагається дістатись шкідливе програмне забезпечення. Проте, в системі інколи лишаються старі файли, що уповільнюють систему, та надають фору зловмисникам, тож інколи необхідно видаляти надто старі файли для забезпечення швидкодії системи.

Також варто згадати про резервні копії системи, на випадок збоїв з боку технічної сторони. Резервні копії мають бути не підключені до мережі, проте окремо слід зауважити, що інколи



роблять тест-сервер, на якому тестують усі оновлення та програмні засоби, а вже потім додають на основний.

При дотриманні таких мінімальних систем захисту можна зменшити ризик втручання в роботу серверу до мінімально можливого. Проте для захисту від DDoS-атак можна використати перенаправлення трафіку та його блокування, для зменшення навантаження на один сервер. Для цього використовується розподілена обчислювальна мережа, що може містити багато серверів або персональних комп'ютерів, що з'єднані віртуальною або локальною мережею. Саме завдяки такому підходу можна зменшити навантаження на одну одиницю обчислювальної техніки та рівномірно розподілити навантаження серед усіх.

На відміну від України, де існують закони загального призначення, що захищають людину та її дані в кіберпросторі, в ЄС існує GDPR.

**Загальний регламент про захист даних** (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) — регламент у межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Вона також стосується експорту персональних даних за межі ЄС і ЄЕЗ. GDPR покликаний насамперед надати громадянам і резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання у межах ЄС.

Захист даних за призначенням і за замовчуванням (ст. 25) вимагає, щоб захист даних був частиною розробки бізнес-процесів, продуктів і послуг. Налаштування конфіденційності, таким чином, повинні бути встановлені на високому рівні за замовчуванням, і контролер має здійснити технічні та процедурні заходи, щоб забезпечити дотримання регламенту впродовж усього життєвого циклу опрацювання даних. Контролери повинні також упровадити механізми, які гарантують, що персональні дані не опрацьовуються, якщо не є необхідні для кожної конкретної мети [5].

Кажучи про GDPR, що наразі не дуже розповсюджений у кіберпросторі України, можна сказати, що його не дотримуються велика кількість установ і критичних об'єктів інфраструктури. Наразі це робить персональні дані всіх користувачів таких систем менш захищеними від несанкціонованого використання як зловмисниками так і самими установами. Використовуючи GDPR у системі цифрової освіти, можливо надати доступ користувачу на відслідковування своїх персональних даних, що робить користувача більш обізнаним та менш вразливим до обману.

**Висновок.** Як висновок, можна сказати, що цифровізація освіти — це один з найважливіших етапів розвитку України, оскільки впливає на підготовку нових кадрів, які будуть здатні працювати у цифровому світі. Неможливо виключити ситуації зі спробами отримання несанкціонованого доступу, тому питання захисту персональних даних є актуальною проблемою інформаційної безпеки. Саме тому необхідно розуміти основні способи завдати шкоди системі та методи попереднього захисту від них. Також, як приклад було розглянуто та проаналізовано приклад Європейського регламенту захисту інформації, та пояснено необхідність введення регламенту у кіберпростір України.

### *Література*

1. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження КМУ від 17.01.2018 р. № 67-р // Офіційний вісник України від 23.02.2018 — 2018 р., № 16, стор. 70, стаття 560, код акта 89147/2018.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017 року № 2163-VIII // Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403 (Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241)

3. Про інформацію: Закон України від 02.10.1992 року N 2657-XII // Відомості Верховної Ради України від 01.12.1992 — 1992 р., № 48, стаття 650.

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 року N 80/94-ВР // Відомості Верховної Ради України від 02.08.1994 — 1994 р., № 31, стаття 286.

5. Загальний регламент про захист даних [Електронний ресурс]. — Режим доступу: [https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9\\_%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82\\_%D0%BF%D1%80%D0%BE\\_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82\\_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85](https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82_%D0%BF%D1%80%D0%BE_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85). — Назва з екрану.

6. The Open Source Security Testing Methodology Manual (OSSTMM). [Електронний ресурс]. — Режим доступу: <https://www.isecom.org/OSSTMM.3.pdf> (дата звернення: 20.12.2019).

7. Певнев В.Я., Цуранов М.В. Математическая модель информационной безопасности. Системы обработки информации. 2010. № 3. С. 62–64.

8. Певнев В.Я. Методы обеспечения целостности информации в инфокоммуникационных системах. Вісник Національного технічного університету ХПІ. Серія: Техніка та електрофізика високих напруг. Харків, 2015. № 51. С. 74–77.

9. SMART-ТЕХНОЛОГІЇ ТА ЇХ ЗАСТОСУВАННЯ В НАВЧАЛЬНОМУ ПРОЦЕСІ: ЕВОЛЮЦІЯ, СУЧАСНІ ТРЕНДИ ВІТЧИЗНЯНОГО ТА ЗАРУБІЖНОГО ДОСВІДУ [Електронний ресурс] Режим доступу: <https://knute.edu.ua/file/NjY4NQ==/4ce2164e98881e82955393871be6013d.pdf> — Назва з екрану.

## References

1. Kontsepsiia rozvytku tsyvrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii: Rozporiadzhennia KМУ vid 17.01.2018 r. № 67-r // Ofitsiyni visnyk Ukrainy vid 23.02.2018 — 2018 r., № 16, stor. 70, stattia 560, kod akta 89147/2018.

2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5.10.2017 roku № 2163-VIII // Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st.403 (Iz zminamy, vnesenyi zghidno iz Zakonom № 2469-VIII vid 21.06.2018, VVR, 2018, № 31, st.241).

3. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 roku N 2657-XII // Vidomosti Verkhovnoi Rady Ukrainy vid 01.12.1992 — 1992 r., № 48, stattia 650.

4. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh: Zakon Ukrainy vid 05.07.1994 roku N 80/94-VR // Vidomosti Verkhovnoi Rady Ukrainy vid 02.08.1994 — 1994 r., № 31, stattia 286.

5. Zahalnyi rehlyment pro zakhyst danykh [Elektronnyi resurs]. — Rezhym dostupu: [https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9\\_%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82\\_%D0%BF%D1%80%D0%BE\\_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82\\_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85](https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82_%D0%BF%D1%80%D0%BE_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85). — Nazva z ekranu.

6. The Open Source Security Testing Methodology Manual (OSSTMM). [Elektronnyi resurs]. — Rezhym dostupu: <https://www.isecom.org/OSSTMM.3.pdf> (data zvernennia: 20.12.2019).

7. Pevnev V.Ia., Tsuranov M.V. Matematycheskaia model informatsyonnoi bezopasnosti. Systemy obrobky informatsii. 2010. №3. S. 62–64.

8. Pevnev V.Ia. Metody obespechenyia tselostnosti ynformatsyy v ynfokommunikatsyonnykh systemakh. Visnyk Natsionalnoho tekhnichnoho universytetu KhPI. Serii: Tekhnika ta elektrofizyka vysokykh napruh. Kharkiv, 2015. № 51. S. 74–77.

9. SMART-ТЕХНОЛОГІЇ ТА ЇХ ЗАСТОСУВАННЯ В НАВЧАЛЬНОМУ ПРОЦЕСІ: ЕВОЛЮЦІЯ, СУЧАСНІ ТРЕНДИ ВІТЧИЗНЯНОГО ТА ЗАРУБІЖНОГО ДОСВІДУ [Elektronnyi resurs] Rezhym dostupu: <https://knute.edu.ua/file/NjY4NQ==/4ce2164e98881e82955393871be6013d.pdf> — Nazva z ekranu.

Статтю подано до редакції 04.10.2019 р.