УДК 004.056
DOI: 10.31673/2409-7292.2022.031823

Звєздогляд О.В., Шевченко Р.Ю.

ДИНАМІКА ЗМІНИ СИСТЕМ БЕЗПЕКИ У ПРОЦЕСІ РОЗВИТКУ КОМПАНІЇ ВІД МАЛОЇ ДО ВЕЛИКОЇ

Стаття присвячена вивченню особливостей управління інформаційною безпекою компанії у процесі її розвитку від малої до великої. Вивчено загальні визначення та теоретичні положення інформаційної безпеки; досліджено сучасний стан і тенденції розвитку СУІБ малого, середнього та великого бізнесу в Україні; розроблено моделі забезпечення ІБ для малих, середніх та великих компаній і дано обгрунтовані рекомендації щодо їх впровадження. Результати дослідження можуть бути використані на підприємствах та організаціях малого, середнього та великого бізнесу у процесі вирішення проблем ІБ, запобігання виникненю критичних помилок, інцидентів та зайвих витрат в процесі зростання та розвитку бізнесу від малого до великого.

Ключові слова: управління інформаційною безпекою, система управління інформаційною безпекою, особливості управління інформаційною безпекою малого, середнього й великого бізнесу.

Вступ

Однією з найважливіших складових успішного розвитку підприємства є захищеність його інформаційних ресурсів. Водночас у зв'язку зі зростаючою складністю інформаційних систем та інформаційних технологій, що використовуються в них, зростає і кількість потенційних загроз цим системам. Нині із загрозами інформаційної безпеки стикається понад 90% компаній, третина кібератак закінчується втратою важливої для бізнесу інформації [1]. Питання забезпечення інформаційної безпеки на сучасному етапі є вкрай важливими для малого, середнього та великого бізнесу в українській державі, оскільки загрози інформаційній безпеці досить динамічні і постійно змінюються. З огляду на щойно викладене, питання розробки та вдосконалення процесів управління інформаційною безпекою бізнесу мають велике науково-практичне значення.

Мета роботи полягає у вивченні особливостей управління інформаційною безпекою компанії у процесі її розвитку від малої до великої.

Моделі забезпечення інформаційної безпеки для малих, середніх та великих компаній

Для кожного бізнесу, особливо малого, в силу зрозумілих обмежень сфери діяльності та особливості бізнесової структури окремо-взятої компанії неможливо створити єдину уніфіковану, прийнятну для всіх модель ІБ. Проте, якщо під моделлю розуміти список рекомендацій, який з більшою ймовірністю може бути імплементований до широкого кола бізнесових структур різних напрямків економічної діяльності, то така задача вбачається цілком реалістичною.

Так, приклад, розроблена модель ІБ Cisco [2] для малого бізнесу є самодостатньою добре організованою та збалансованою системою засобів забезпечення ІБ, при можливості імплементації якої ймовірність інцидентів ІБ значно скорочується. Проте, беручи до уваги всі документи стандартизації ІБ та моделі її імплементації, в умовах українського бізнесу, слід розуміти, що вони розроблені, в першу чергу, для закордонного користувача, що створює певну невідповідність між матеріальними та фінансовими можливостями закордонних та українських компаній. Таким чином, ми будемо формувати рекомендації із забезпечення ІБ малого бізнесу, виходячи з позиції розуміння обмеженості матеріальних, фінансових та кадрових ресурсів, з урахуванням потреб та проблем ІБ саме малого бізнесу. Що в свою чергу приводить до вибору методу забезпечення ІБ, а саме – **фрагментарного підходу**.

Дотримання елементарної **інформаційної гігієни** є обов'язковим завжди. У малих компаніях навчання співробітників часто ігнорується з боку керівництва, проте розуміння того чи здатні співробітники, до прикладу, відрізнити лист зловмисника з шифрувальником від листа контрагента з необхідною документацією (фішинг), чи можуть вони видати свої паролі людині, яка представилася фахівцем техпідтримки банку, є цілком реальною потребою сьогодення як для бізнесу, так і для окремої особи.

© Звєздогляд О.В., Шевченко Р.Ю., 2022

Розподілений доступ до інформаційно-виробничих ресурсів в цілому та управління ПЗ зокрема є невід'ємною вимогою ІБ сьогодення. Проблематика неналежного керування правами адміністратора дає вичерпну відповідь у необхідності використання такого підходу в будь-яких бізнес-процесах. Іншим шляхом реалізації технічної підтримки ПЗ бізнесу є **аутсорсинг**, з огляду на що не можемо однозначно рекомендувати таке рішення саме в сфері ІБ. Але, якщо розуміти під аутсорсингом, наприклад, надавачів послуг з хостингу, DaaS, SaaS, Cloud, VDS/VPS [3] тощо, то це є більш прийнятним та рекомендованим рішенням, оскільки задачі по забезпеченню ІБ, в сенсі надання засобів розподіленого доступу, зберігання інформації, протидії DDOS-атакам тощо, лежать в межах компетенції компанії-надавача таких послуг та керуються, як правило, положеннями публічної оферти відповідно до законів України. Тобто, що **хмарний сервіс** самостійно несе відповідальність за цілісність, доступність та конфіденційність даних і захист не від внутрішніх загроз (співробітників компанії), а саме від зовнішніх атак, обумовлених положеннями договору.

Універсальні рішення є менш гнучкими та зручними у використанні, що теж веде до підвищення навантаження на співробітників, збільшення необхідного рівня їх компетентності та відповідальності, і, як результат, зростання ризику помилки. Альтернативою є використання **демо-ліцензій** необхідного ПЗ [4], після завершення терміну якої, як правило, таке ПЗ не втрачає повністю своїх можливостей, а лише певної їх частини, що за умови достатності функціоналу для забезпечення потреб окремого взятого малого бізнесу, є цілком виправданим і відповідає критерію ефективності ІБ у стані необхідності мінімізації витрат. Окремою складовою ІБ малого бізнесу є **фізична безпека**, яка полягає в організації та забезпечені чинників запобігання фізичному доступу до інформації чи носіїв інформації (співробітників), як то системи відеоспостереження, системи розподілення доступу до приміщень, смарт-карти та USB-ключі для автентифікації користувачів тощо.

Отже, після аналізу активів та пов'язаних ризиків власники чи керівники малого бізнесу мають забезпечити створення **політики інформаційної безпеки,** в якому обліковано активи, проаналізовано ризики та вказано засоби, методи і протоколи забезпечення ІБ, прийняті в окремо взятій бізнесовій структурі. Такий документ в більшості випадків взагалі відсутній у представників малого бізнесу, тому що розглядається як необов'язковий. Проте сама його відсутність здебільшого і стає фундаментом для інцидентів ІБ.

Таким чином, рекомендації щодо ІБ малого бізнесу можуть бути узагальнені у вигляді наступної схеми (рис. 1)

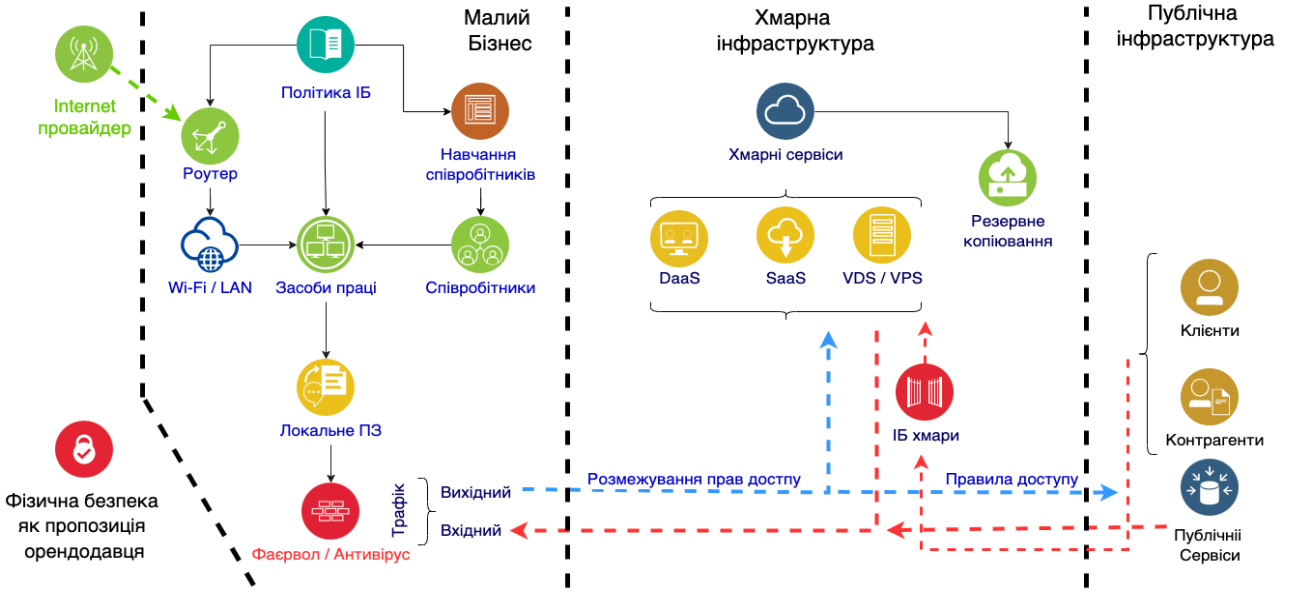

Рис. 1. Орієнтовна модель ІБ малого бізнесу

© *Звєздогляд О.В., Шевченко Р.Ю., 2022*

Концепція інформаційної безпеки середнього бізнесу як результат розвитку

Кожен бізнес у процесі свого розвитку проходить певні етапи, що можуть характеризуватись різними стратегічними підходами, технологіями, підвищенням рівня управлінської діяльності, ростом компетентності персоналу й іншими якісними та кількісними ознаками. Перехід на кожен наступний, більш високий рівень розвитку здійснюється шляхом покращення показників діяльності організації при позитивній динаміці ключових характеристик, що робить організацію більш конкурентоспроможною, покращує можливість динамічного реагування на нові фактори та оптимального використання своїх внутрішніх ресурсів.

Це, в свою чергу, знову приводить до вибору методу забезпечення ІБ, а саме – **фрагментарного підходу**, зі збільшенням рівня тяжіння до **комплексності**. Комплексний підхід поєднує в одне ціле окремі методи та засоби забезпечення ІБ, що в свою чергу дозволяє гарантувати високий рівень захисту на всіх рівнях доступу до інформації. Зі зростанням кількості кадрів внутрішні загрози стають ключовою проблемою середнього бізнесу, оскільки вони є основним джерелом інцидентів ІБ.

Крім того, світова тенденція BYOD – Принеси Свій Прилад є одночасно як проблемою ІБ, так і рішенням бізнесових задач в умовах обмеженості ресурсів. Ця проблема посилюється, якщо працівник провадить роботу поза межами фізичного периметру безпеки, скажімо, офісу. У рамках концепції BYOD більшість віртуальних рішень для мобільних пристроїв можна віднести до двох класів залежно від варіанту технічної реалізації та політики ІБ компанії:

1. Віртуальний робочий стіл (VDI та подібні рішення)

Рішення подібне до стандартних рішень корпоративної інфраструктури з тонкими клієнтами: користувач працює в середовищі віддаленого робочого столу, не маючи можливості зберегти щось на своє локальне робоче місце (тобто пристрій як точка входу в робоче середовище).

2. Хмарна віртуалізація

Хмарний сервіс, який передбачає налаштування на пристрої користувача ярликів доступу до додатків чи програм, у той час, як усі дані зберігаються та обробляються на стороні хмарного хостингу, в якому відбувається також розмежування доступу до програм та управління користувачами відповідно до політик ІБ роботодавця.

Отже, з розвитком компанії рекомендована структура ІБ середнього бізнесу може мати такий вигляд (рис. 2):

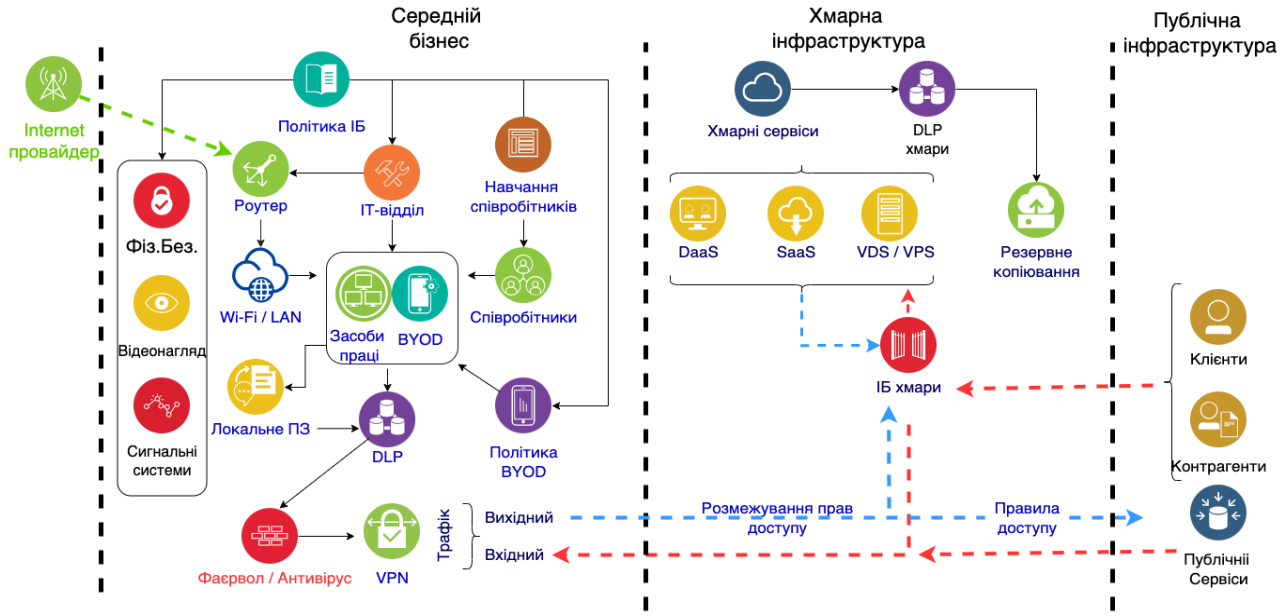

Рис. 2. Орієнтовна модель ІБ середнього бізнесу

© Звєздогляд О.В., Шевченко Р.Ю., 2022

Система управління та автоматизація інформаційної безпеки великого бізнесу – результат попереднього досвіду управління інформаційною безпекою

Головною ознакою сучасного бізнесу можна назвати його залежність від інформації, повсюдну інформатизацію бізнес-процесів, що, у свою чергу, передбачає активне використання цілої низки підсистем інформаційної безпеки. Розвиток засобів, методів та систем забезпечення ІБ, особливо у великому бізнесі, призводить до практики застосування значної кількості різних технічних систем та засобів захисту інформації (СЗІ) у поєднанні з організаційно-технічними засобами реалізації моніторингу та контролю заходів ІБ, розслідувань за виявленими інцидентами. Загалом, автоматизація ІБ реалізується у вигляді програмно-технічної надбудови, яка дозволяє автоматизувати більшість функцій управління ІБ і має ряд вбудованих модулів, що забезпечують вирішення певного окремого завдання з її забезпечення.

Найчастіше типова структура системи автоматизованого управління ІБ має трирівневу архітектуру:

1) Перший рівень – збір, обробка та передача на наступний рівень зібраної інформації щодо подій ІБ. Збір інформації надходить від усіх систем та засобів забезпечення ІБ, системного та прикладного ПЗ, серверів, мережевого обладнання, засобів антивірусного захисту, міжмережевих екранів тощо.

2) Рівень обробки інформації – аналіз та кореляція подій та інцидентів, що надходять від попереднього рівня.

3) Рівень управління – власне автоматизації процесу управління – є адаптивним інтерфейсом, що дозволяє в режимі реального часу управляти інцидентами ІБ, проводити аналіз стану, видавати звіти і рекомендації щодо стану ІБ загалом і окремих систем безпеки зокрема.

Крім підвищення ефективності ІБ бізнесу впровадження та подальше використання автоматизованих систем управління також дозволяє виконати вимоги великої кількості міжнародних стандартів ІБ, зокрема значної частини вимог групи стандартів з ІБ ISO/IEC 27000 [5].

Фізична безпека, у випадку середнього, а особливо малого, бізнесу могла мати другорядне значення в забезпеченні ІБ як з огляду на можливу специфіку сфери діяльності того чи іншого бізнесу, так і як невиробнича складова, що може бути додатковою пропозицією, наприклад, орендодавця виробничого приміщення. У випадку з великим бізнесом при імплементації СУІБ, фізична складова ІБ не може ігноруватися чи, навіть, забезпечуватися фрагментарно.

Нормативне забезпечення. Розроблений, задукоментований та оновлюваний документ з політиками фізичного захисту периметру ІБ.

Персонал та рівні доступу. Вичерпний перелік працівників (включно з власниками та директорами), який змінюється та переглядається відповідно з фактами зміни статусу співробітника (прийняття/звільнення/зміна посади тощо) з переліком доступів до інформації та засобів ідентифікації: бейджі; цифрові картки доступу; смарт-ключі; біометричні сканери та профілі тощо.

Управління фізичним доступом. Встановлений пропорційно до можливих загроз рівень забезпечення фізичного доступу до периметру ІБ, який:

має систему управління доступом у всіх точках доступу до інформаційних ресурсів та активів;

використовує чітко визначені периметри безпеки для захисту приміщень та зон, у яких розташовані засоби обробки інформації;

забезпечує доступ до приміщень та будівель лише авторизованому персоналу;

забезпечує перевірку повноважень та доступів перед забезпеченням фізичного доступу до активів бізнесу;

Моніторинг фізичного доступу. Рівень фізичної безпеки, який забезпечує контроль фізичного доступу до приміщень у процесі моніторингу в режимі реального часу з

© Звєздогляд О.В., Шевченко Р.Ю., 2022

використанням методів ідентифікації/автентифікації відповідно до політики ІБ за допомогою програмно-технічних засобів, як наприклад:

пристрої відео-спостереження;

сигналізації;

автоматизовані засоби, які забезпечують розпізнання порушень тощо.

Захист обладнання:

специфікація правил розміщення обладнання таким чином, щоб зменшити ризики від впливів з навколишнього середовища та можливості неавторизованого доступу;

правила захисту від перебоїв у подачі електроенергії та інших збоїв, пов'язаних з електрикою (резервні джерела живлення, генератори тощо);

правила забезпечення протипожежного захисту, екологічних та техногенних катастроф тощо;

правила захисту телекомунікаційних кабельних мереж від перехоплення інформації чи пошкодження;

регламентація проведення належного технічного обслуговування обладнання для забезпечення його безперервної працездатності та цілісності.

Контроль відвідувачів:

передбачає уніфіковані виділені зони реєстрації відвідувачів;

регламентує правила перебування та супроводу відвідувачів на об'єктах периметру ІБ;

правила ведення журналів обліку/доступу відвідувачів;

регламентація періодичного аналізу журналів обліку/доступу відвідувачів відповідними посадовими особами.

Таким чином, пропонована система ІБ великого бізнесу може мати наступний вигляд (Рис. 4), з поправкою на специфіку самого бізнесу. Окремо слід зазначити, що попередньо розглянуті та запропоновані системи ІБ для малого та середнього бізнесу можуть бути органічно вбудовані в інфраструктуру ІБ великого бізнесу як керовані складові його віддалених офісів.

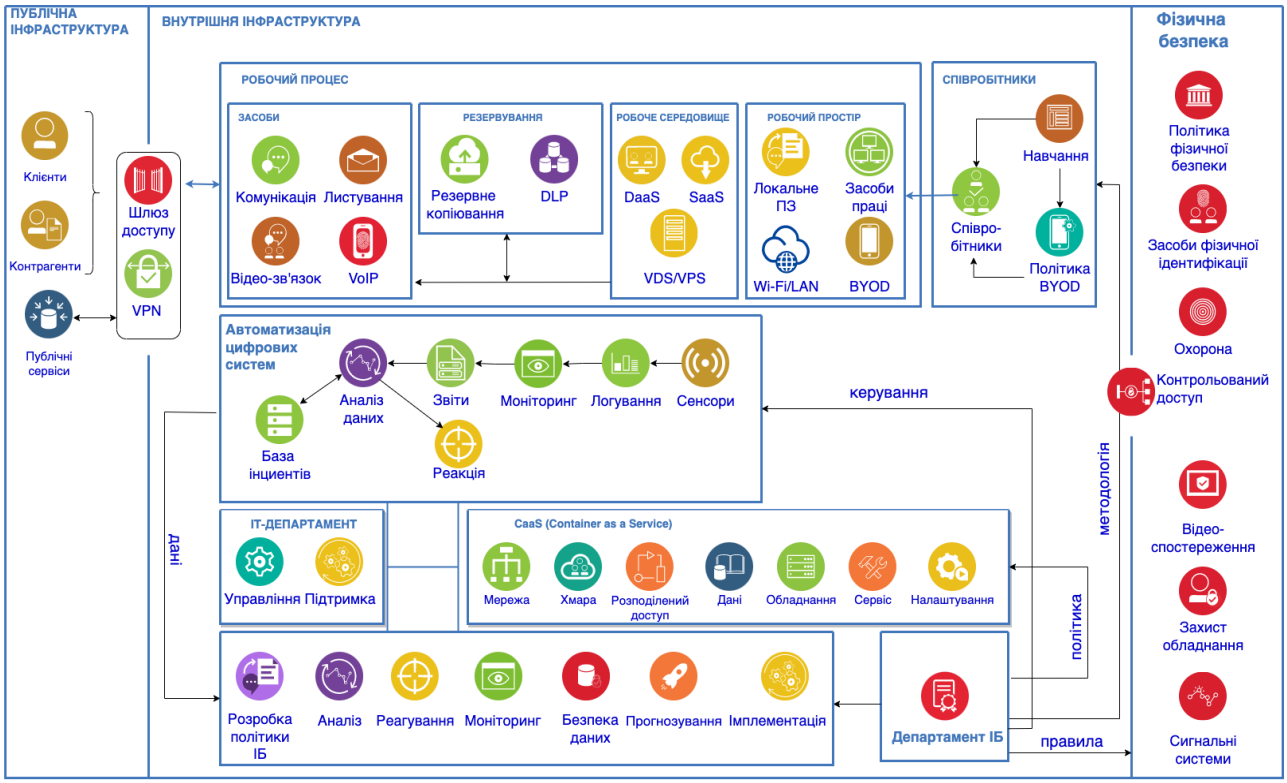

Рис. 4. Орієнтовна модель ІБ великого бізнесу

© *Звєздогляд О.В., Шевченко Р.Ю., 2022*

Висновки

Для кожного бізнесу створити єдину уніфіковану, прийнятну для всіх модель ІБ неможливо. Кожний бізнес у процесі свого розвитку проходить певні етапи, і за умови, що фундамент інформаційної безпеки компанії був закладений правильно з самого початку з дотриманням «інформаційної гігієни», перехід на кожен наступний, більш високий рівень розвитку для підприємства проходить набагато легше та плавніше, ніж у конкурентів у тій же сфері. Чим краще було відбудовано мінімальну частину ІБ, тим легше і дешевше в подальшому відбувається розвиток бізнесу. Для великого бізнесу стає актуальним об'єднання всіх застосовуваних захисних заходів у єдиний, адекватний реальним загрозам, адаптивний комплекс, що дозволяє досягати необхідного рівня ІБ за допомогою засобів автоматизації та візуалізації наданої інформації згідно з політикою ІБ компанії. У контексті комплексного підходу до ІБ проведена за умов обмеженості ресурсів попередня підготовка під час практики керування ІБ малого та середнього бізнесу може бути повністю імплементована та розширена на розгалужену систему ІБ великого підприємства в складі повноправного учасника СУІБ.

Перелік посилань

1. 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends. URL: https://purplesec.us/resources/cyber-security-statistics (Дата звернення: 19.03.2022)
2. Celia Paulsen Patricia Toth, Small Business Information Security: The Fundamentals. URL:
3. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf (Дата звернення: 19.04.2022)
4. The most in-demanded Cyber skills for 2022. URL: https://www.infosecurity-magazine.com/blogs/in-demand-cyber-skill-2022 (Дата звернення: 18.06.2022)
5. Free SANS Information Security Resources: https://www.sans.org/security-resources (Дата звернення: 15.05.2022)
6. ISO/IEC 27000:2018 / Information technology – Security techniques – Information security management systems – Overview and vocabulary. 2018. 27 p.
7. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки [Текст] : ДСТУ (Державний стандарт України) / Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20). – Київ: ДП «УкрНДНЦ», 2018. – 44 с.
8. Мужанова, Т. М. Інформаційна безпека держави [Текст] : Навчальний посібник / Т. М. Мужанова. – Київ: Державний університет телекомунікацій, 2019. – 131 с.
9. Santos, H. M. D. Cybersecurity: A Practical Engineering Approach [Text] : Monograph / H. M. D. Santos. – CRC Press, 2022. – 340 p.
10. Yevseiev, S. Synergy of building cybersecurity systems [Text] : Monograph / S. Yevseiev [et al.]. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
11. James, A. IoT System Design: Project Based Approach [Text] : Monograph / A. James, A. Seth, S. C. Mukhopadhyay. – Springer, 2022. – 291 p.

Надійшла: 21.08.2022 Рецензент: д.т.н., професор Гайдур Г.І.

© Звєздогляд О.В., Шевченко Р.Ю., 2022