ВСТУП

Запропонована комплексна лабораторна робота відображає сучасні погляди на основи менеджменту інформаційної безпеки (ІБ) підприємства та орієнтована на підготовку фахівців за спеціальністю 125 «Кібербезпека та захист інформації». Робота призначена для майбутніх фахівців з менеджменту інформаційної безпеки загалом та інформаційних ризиків зокрема у стрімко плинному навколишньому світі бізнес-процесів та інформаційних технологій, в якому не працюють правила минулого століття, переглядаються основи ведення бізнесу, економічні закони та людські цінності, а *інформація стала найголовнішим та найуразливішим активом.*

Безперечно, результати та висновки цієї лабораторної роботи будуть цікавими для майбутніх фахівців у галузі ІБ, зокрема менеджерів, аудиторів, експертів, аналітиків, інженерів, а також всіх тих, хто:

– розробляє та впроваджує політику ІБ;

– ухвалює рішення з питань ІБ та її фінансування;

– запроваджує системи управління ІБ і/або готує підприємство до сертифікації за вимогами міжнародного стандарту ISO 27001;

– має стосунок до оцінювання та управління інформаційними ризиками підприємства;

– здійснює планування заходів з ІБ та розставляє пріоритети;

– формує та обґрунтовує бюджет на ІБ;

– бере участь у плануванні та проведенні аудитів ІБ;

– оцінює економічну ефективність та необхідність реалізації заходів захисту.

Автори також сподіваються, що результати та висновки цієї лабораторної роботи будуть цікавими та корисними для тих, хто бажає:

– взяти під контроль ризики інформаційної безпеки в усіх галузях діяльності;

– формувати стратегію і тактику планування та запровадження режиму ІБ організації;

– розширити та поглибити власне розуміння змісту процесів забезпечення ІБ;

– перейти від *міркувань* про зв'язок бізнесу, інформаційних технологій та безпеки до *реальних дій* з управління цими складниками.

Виконання лабораторної роботи допоможе систематизувати наявні знання та перейти до створення ефективної системи управління ІБ завдяки оволодінню навиками управління інформаційними ризиками, знання про які є фундаментом для розроблення політики безпеки, які відповідають вимогам його підприємства. Новачку вона дасть змогу отримати базовий набір знань, потрібних для того, щоб забезпечити успішний старт у сфері менеджменту ІБ.

Оскільки **студент <u>самостійно</u> формує ту чи іншу власну систему знань**, то ***головна мета*** комплексної лабораторної роботи – ознайомити студентів із *логікою найкращих світових практик* та показати *сучасні підходи запровадження системи менеджменту ІБ організації*, зокрема, *системні ризик-орієнтовані підходи, методики оцінювання ризиків* та *повернення інвестицій* в інформаційну безпеку, розроблення та впровадження *політик ІБ.*

Основну увагу під час виконання комплексної лабораторної роботи зосереджено на понятті менеджменту ІБ у контексті взаємодії співробітників, бізнес-процесів, підприємств, а не лише управління, коли передбачається взаємодія програмно-технічних засобів.

У проблемі менеджменту ІБ є два ключові аспекти: *управління інформаційними ризиками* та *управління доступом*. Тож, якщо проблема управління доступом широко висвітлена у літературі, то проблема управління інформаційними ризиками є порівняно новим напрямом наукових досліджень в Україні, а тому на ринку майже немає навчально-наукової літератури вітчизняних авторів із вказаної проблеми.

Управління інформаційними ризиками – тема для багатьох неочевидна, однак її значення у житті суспільства зростає. Уже невдовзі вона вийде на перший план поряд з політичними, фінансовими або військовими подіями. А тому політикам, бізнесменам, військовим, керівникам різних рівнів, а також усім спеціалістам, які пов'язані з інформаційними технологіями, важливо

підготувати власну свідомість до сприйняття нових реалій та розв'язання незнаних раніше проблем, пов'язаних із загрозами інформаційної безпеки.

Вказана сфера діяльності асоціюється у масовій свідомості з хакерами та комп'ютерними вірусами, а також з витоком даних. Насправді *інформаційна безпека є на стику загального менеджменту організації, інформаційних технологій, фізичної безпеки та психології*. Для успішного розв'язання проблем ІБ потрібні нетрадиційні підходи, а також суміщення знань з різних технічних і гуманітарних ділянок, які важко поєднати в одній людині. А упираються усі ці непрості питання у кінцевому підсумку ***в управління ризиками***.

З другого боку, управління ризиками є лише одним із ключових аспектів ІБ організації, який створює підґрунтя, аналітичну базу для формулювання *стратегії і тактики* планування та впровадження методів і засобів захисту. Тож стратегія і тактика ІБ організації і є ***політикою інформаційної безпеки організації***. Водночас розрізняють *загальну стратегічну політику інформаційної безпеки*, взаємопов'язану зі стратегією розвитку бізнесу та стратегією організації, а також *часткові тактичні політики безпеки*, які деталізують вимоги ІБ під час роботи з відповідними її інформаційними активами, системами та службами тощо.

Актуальність розроблення політик ІБ для вітчизняних організацій пояснюється потребою формування основ планування інформаційної безпеки та управління нею на сучасному етапі. Сьогодні більша частина українських організацій визначила такі пріоритетні завдання розвитку та вдосконалення своєї діяльності:

– мінімізація ризиків бізнесу за допомогою захисту власних інтересів в інформаційній сфері;

– забезпечення безпечного, довірливого та адекватного управління організацією;

– планування та підтримання неперервності бізнесу;

– підвищення якості заходів із забезпечення ІБ;

– зменшення видатків та підвищення ефективності інвестицій, зокрема, в ІБ;

– підвищення рівня довіри в акціонерів, потенційних інвесторів, ділових партнерів, учасників ринку цінних паперів та інших зацікавлених сторін.

Водночас успішне виконання перелічених завдань в умовах внутрішніх та зовнішніх факторів, а також дій конкурентів і зловмисників є доволі проблематичним. Це пов'язано із все більшою потребою підвищення рівня ІБ та недостатнім рівнем опрацювання політик інформаційної безпеки у вітчизняних організаціях, що зумовлено не в останню чергу недостатнім фаховим рівнем працівників цієї галузі.

Запропонована комплексна лабораторна робота покликана частково зняти наявну на ринку проблему фахової **популяризації** *найкращих світових підходів запровадження систем менеджменту інформаційною безпекою організації*. Зазначимо, що термін *організація* має інтегральний, узагальнювальний характер без розкриття організаційної структури та структури власності для низки інших, зокрема, підприємства, установи, корпорації, компанії, фірми тощо.

Виконання комплексної лабораторної роботи має **надзавдання**. Важливо донести одну, на перший погляд, просту істину: ***власники створюють підприємства не як об'єкти для запровадження інформаційних технологій, а як структури для досягнення мети, зокрема, у випадку комерційних проєктів – для отримання прибутку***. Запровадження підприємством інформаційних технологій може примножити прибуток. За такого підходу *ІБ повинна працювати на підприємство* для забезпечення досягнення мети. А тому результат роботи *служби ІБ є* лише вхідною інформацією для керівництва підприємства під час ухвалення управлінських рішень для отримання максимального результату у процесі реалізації мети.

Досвід показує, що фахівець, який набув теоретичних знань з питань ІБ, лише тоді *буде цінуватися на ринку інформаційних технологій*, якщо він, з одного боку, *усвідомить свої роль і місце* в підприємстві, а з другого – набуде практичних навиків роботи на *взірцях кращих світових практик менеджменту інформаційної безпеки*. Можемо стверджувати, що **оволодіння практичними навиками побудови системи менеджменту ІБ підприємства на основі системних ризик-орієнтованих підходів є гарантією успішного працевлаштування** у провідних вітчизняних та зарубіжних бізнес-підприємствах, органах влади та контролю тощо.