of entrepreneurial culture of graduates of the faculties of physical education and sports on the basis of the factor-criterion model developed a textbook, the answers to which correspond to a certain level of entrepreneurial culture on a five-point scale. The proposed diagnostic tool will not only assess the general level of entrepreneurial culture of respondents, but also identify the most problematic parameters, which can be further used to develop a structural and functional model of entrepreneurial culture and the content of scientific and methodological support of the educational process.

***Key words**: business culture, factor-criterion model, component, element, qualimetric approach, weighting factor, point evaluation, weighted evaluation.*

УДК 378:004.45:0.04.91

Сергій Воскобойников
Національна академія Служби Безпеки України
ORCID ID 0000-0002-5863-5880
Олег Решетніков
Національна академія Служби Безпеки України
ORCID ID 0000-0002-3792-4640
DOI 10.24139/2312-5993/2020.08/095-106

ПРОЄКТУВАННЯ ОСВІТНЬОГО ПРОЦЕСУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ДО УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

У статті здійснено теоретичний аналіз, узагальнено результати дослідження проблеми організації підготовки фахівців управління інцидентами інформаційної та кібербезпеки. Для забезпечення якісного освітнього процесу формування професійної компетентності з управління інцидентами інформаційної та кібернетичної безпеки здійснено обґрунтування, проєктування й розробку навчально-методичного комплексу «Управління інцидентами інформаційної і кібернетичної безпеки». Для педагогічного супроводу формування компетентності управління інцидентами як складові НМК розроблено методичні рекомендації до виконання задач кейсів модельних ситуацій із моніторингу інцидентів інформаційної та кібернетичної безпеки; навчально-інформаційну платформу для віддаленого доступу для проведення семінарських занять у режимі вебінарів, онлайн-конференцій за розділами навчального модулю; методичні рекомендації до виконання лабораторних та самостійних робіт і виконання індивідуальних творчих завдань, проєктування, моделювання тощо.

***Ключові слова:** інформаційна безпека, кібербезпека, освітній процес, формування компетентності управління інцидентами інформаційної та кібернетичної безпеки, навчально-методичний комплекс.*

Постановка проблеми. В умовах інформаційного суспільства реалізація будь-яких процесів неможлива без інформаційного

забезпечення, зокрема інформаційних систем і мереж. Вимоги інформаційної безпеки відображаються в угодах про забезпечення належного рівня сервісу (Service Level Agreement, SAL), будь-який інцидент, що перешкоджає забезпеченню відповідності вимогам SAL, кваліфікується як інцидент інформаційної безпеки, що несе загрозу інформаційній системі, може призвести до несанкціонованого доступу до інформації, втраті інформації, економічним втратам тощо.

Саме тому формування компетентності з управління інцидентами інформаційної та кібернетичної безпеки є важливою складовою формування професійної компетентності майбутніх фахівців із кібербезпеки в сучасних умовах.

Аналіз актуальних досліджень. Інциденти ІБ спричинені багатьма зовнішніми чинниками (загрозами) та внутрішніми вразливостями сучасних інформаційних і телекомунікаційних технологій (обробки, зберігання, передачі інформації). Складний розподілений характер, багатомодульність, помилки й недоліки в програмно-апаратній архітектурі автоматизованих (інформаційних) систем обробки та зберігання даних, які для інформаційного обміну використовують транспортні послуги вразливих і не завжди достатньо захищених ІКМ, наприклад Internet, – створюють додаткові вразливості та можливості для реалізації загроз ІБ у вигляді інцидентів. Крім того, розвиток таких високих технологій (Hi-Tech), як нанотехнології, робототехніка, сенсорні мережі, радіочастотна ідентифікація, телебіометрія, штучний інтелект, інформаційна зброя, нові засоби впливу тощо, – все це несе за собою нові проблеми, ризики, побічні негативні явища. Тому, незважаючи на своє вирішальне значення, доходять висновку науковці, для розвитку інформаційного суспільства в найближчому майбутньому інформаційно-комунікаційні мережі виявляться слабо захищеними від зловживань, вторгнень, зовнішніх і внутрішніх впливів, стаючи ареною інформаційних війн, діяльності кіберзлочинців і Hi-Tech-хакерів. Для інформаційної та національної безпеки України це є особливо актуальним у зв’язку з відставанням нашої держави в критичних напрямах Hi-Tech (Гладиш, 2007).

Першим кроком у прийнятті рішень щодо керування інцидентами ІБ повинна бути систематизація та включення до SLA визначень класів інцидентів. Пропонується постійно осучаснювати як закони, методики, так і відповідні інститути в галузі керування інформаційними технологіями та ІБ. Науковці пропонують функціональні схеми щодо

керування інцидентами ІБ в ОТС, відповідні моделі PDCA та процесний підхід, визначений у відповідних міжнародних стандартах ISO/IEC (Гладиш та ін., 2007; Гладиш, 2008).

Узагальненою метою забезпечення інформаційної безпеки (ІБ) організації є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок –запобігання або мінімізація збитку від можливих інцидентів ІБ. Основною задачею процесу управління інцидентами інформаційної безпеки є усунення інцидентів у гранично стислі терміни. У ході процесу управління інцидентами ІБ проводиться виявлення, реєстрація, класифікація й початкова підтримка запитів, а також пошук рішення, його застосування, контроль, інформування і підготовка звітності. Оскільки, як ми вже визначили, інцидентом, у першу чергу, є певна недозволена подія, вона має бути неприпустимою, забороненою. Отже, існує необхідність розробки та затвердження документів, що чітко описують усі дії, які можна виконувати в ІКС і які виконувати заборонено (Гнатюк та ін., 2012).

Процес управління інцидентами інформаційної безпеки, як правило, покладається на службу IT-підтримки, яка обробляє інциденти ІБ (у випадку, якщо така служба існує в організації). Це ще раз доводить факт доцільності розробки єдиної системи управління всіма процесами в компанії, оскільки управління подібними процесами в різних галузях її діяльності часто виконується за однією схемою. Варто також розуміти, що управління інцидентами інформаційної безпеки не попереджує нанесення збитку компанії, проте розслідування інциденту ІБ та своєчасне впровадження превентивних і коригувальних заходів знижує ймовірність його рецидиву. Робота організації без системи управління інцидентами інформаційної безпеки може обернутися низкою неприємностей. У результаті впровадження процесу управління проблемами організація отримує такі важливі й корисні властивості, як якість сервісів, скорочення числа інцидентів та безперервне функціонування. В умовах зростання впливу IT на діяльність сучасних організацій, значна увага приділяється організації підтримки та супроводу IT-систем (Гнатюк та ін., 2012).

Одним із ключових процесів на етапі експлуатації є розслідування інцидентів. Перш ніж перейти до розкриття процесу розслідування інцидентів безпеки, проаналізуємо сутність поняття інцидент інформаційної безпеки. Основним елементом моделі інциденту інформаційної безпеки є інформаційні активи організації, оскільки саме проти них спрямовується

негативна подія або низка небажаних і непередбачених подій інформаційної безпеки, у результаті їх впливу відбувається порушення політики інформаційної безпеки (ПІБ) (Копитін, 2010).

Для зменшення ризику нанесення збитків, пов'язаних із порушенням ІБ, використовуються заходи (організаційні, інженерно-технічні) й засоби (міжмережеві екрани, віртуальні приватні мережі (VPN), системи виявлення вторгнень/системи запобігання вторгненням (IDS/IPS), системи замкнутого телебачення (CCTV) та ін. системи безпеки. Але якою би потужною не була система ІБ, все одно в ній можуть бути уразливості, пов'язані, наприклад, із появою раніше невідомого вірусу (Копитін, 2010). Відомості щодо останніх уразливостей можна отримати на он-лайн службах (http://www.cert.org/vuls/), у стандарті назв уразливостей Common Vulnerabilities and Exposures (CVE), із яким можна ознайомитися на сайті http://cve.mitre.org/cve/.

Формування групи для проведення розслідування, реагування на інциденти ІБ включає визначення осіб, відповідальних за розслідування. У організацій існує три варіанти вирішення даного питання: провести внутрішнє розслідування; звернутися до правоохоронних органів; звернутися до спеціалізованих груп реагування на інциденти ІБ. Під час проведення внутрішнього розслідування організації стикаються з такими проблемами: низька кваліфікація співробітників у питаннях реагування на інциденти ІБ; недостатня кількість співробітників і часу; неможливість отримати необхідну інформацію під час розслідування та ін. Під час вибору другого та третього варіантів слід розуміти, що конфіденційна інформація може стати відомою стороннім організаціям. На підставі необхідності комплексного вирішення завдань захисту державних інформаційних ресурсів у інформаційних та телекомунікаційних системах було вирішено створити в Україні єдину інфраструктуру безпеки. Основними її елементами мають стати: Державний центр безпеки (ДЦБ) інформаційно-телекомунікаційних систем; Центр безпеки українського сегменту мережі Інтернет; Центр антивірусного захисту інформації; Центр сертифікації ключів із забезпеченням чіткої ієрархії управління та єдиними технологічними принципами створення й функціонування. Єдина інфраструктура безпеки забезпечує взаємодію з адміністраторами безпеки інформаційних систем органів державної влади (Копитін, 2010).

Гарантією безпечної роботи з інформаційної системи є виконання необхідних заходів, які зводять до мінімуму всі існуючі ризики з

урахуванням їх ступеня впливу на безпеку. Ці вимоги визначаються необхідністю врахування всіх ризиків і інтересів, що виникають у процесі впровадження нових інформаційних технологій. Одним зі шляхів вирішення є побудова моделей створення й оцінки ефективності систем безпеки, що забезпечують безпеку на основі системного підходу до врахування впливу ризиків. Для визначення необхідного комплексу заходів проєктують і розробляють модель системи безпеки. Компанії, що мають стратегії кібербезпеки, повинні гарантувати, що кожна з підкатегорій кібербезпеки буде врахована (Стефурак та ін., 2020).

Сьогодні кіберзахист не може обмежуватися технічними заходами, а має бути інтегрований у такі традиційні види діяльності з безпеки, як забезпечення фізичної безпеки та безпеки персоналу, бути частиною загально-організаційних зусиль із метою захисту всіх бізнес-операцій як від зовнішніх, так і від внутрішніх загроз. Активності з кібербезпеки мають бути в числі пріоритетних та узгоджуватися зі стратегічною діяльністю бізнесу. Зростанню ефективності забезпечення кібербезпеки сприяють технології геоінформаційних систем (ГІС), які формують основу для створення спільної ситуаційної обізнаності фахівців із міждисциплінарних видів діяльності в межах організації. ГІС – це автоматизована система, що забезпечує збирання, зберігання, інтеграцію та графічне представлення просторової інформації у вигляді схем або карт. Більшість сучасних ГІС здійснюють комплексну обробку інформації, з використанням функцій: уведення й редагування даних, підтримка моделей просторових даних, зберігання інформації, перетворення систем координат і трансформація картографічних проєкцій, растрово-векторні операції, вимірювальні операції, полігональні операції, операції просторового аналізу, різні види просторового й цифрового моделювання (Мужанова, 2020).

Узагальнюючи результати теоретичного аналізу проблеми, визначаємо, що для якісної професійної підготовки майбутніх фахівців важливими є всі розглянуті положенні та їх вивчення й аналіз у проєктуванні навчально-методичного забезпечення для теоретико-методичного супроводу процесу формування компетентності управління інцидентами інформаційної і кібернетичної безпеки.

Мета полягає у здійсненні аналізу наукових джерел, обґрунтуванні, проєктуванні й розробці навчально-методичного комплексу для забезпечення якісного освітнього процесу формування професійної компетентності з управління інцидентами інформаційної та кібернетичної безпеки.

Відповідно до мети визначено завдання дослідження: 1) здійснити теоретичний огляд наукових джерел із управління інцидентами інформаційної та кібернетичної безпеки; 2) здійснити проєктування й розробку навчально-методичного комплексу з управління інцидентами інформаційної та кібернетичної безпеки.

Методи дослідження: базовим стало інтегроване застосування системного, компетентнісного й діяльнісного підходів, використання загальнонаукових та спеціальних методів: системного аналізу та синтезу, термінологічного аналіз, узагальнення. У ході проєктування, розробки й упровадження НМК в освітній процес використано методи навчання: індуктивний, дедуктивний, продуктивний та метод стимулювання; інтерактивні методи: проблемної дискусії; мозкового штурму; проєктування: моделювання; дерева рішень; експертних груп, case-study.

Виклад основного матеріалу. Відповідно до вимог освітньо-професійної (освітньо-наукової) програми та результатів навчання студенти повинні володіти такими компетентностями: здатність управляти інцидентами інформаційної та кібернетичної безпеки відповідно до міжнародних стандартів ISO/AEC 27 серії; здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку; виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем відповідно до встановленої політики інформаційної та/або кібербезпеки; аналізувати, виявляти й оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з установленою політикою інформаційної та/або кібербезпеки; застосувати методи розслідування і аналізу для збору, використання та збереження доказів злочину в кіберпросторі.

Для забезпечення якісного освітнього процесу формування професійної компетентності майбутніх фахівців із кібербезпеки й означених компетентностей, що є її складовими, розроблено навчально-методичний комплекс «Управління інцидентами інформаційної і кібернетичної безпеки».

Теоретична частина включає авторську розробку навчально-методичного комплексу – інформаційний контент лекційних занять за підрозділами: основні поняття, терміни й нормативно-правова база управління інцидентами інформаційної та кібернетичної безпеки; міжнародні стандарти щодо управління інцидентами інформаційної та

кібернетичної безпеки, управління комп'ютерними інцидентами на основі стандартів ISO/AEC 27 серії; основні методи та засоби управління інцидентами інформаційної та кібернетичної безпеки; обробка інцидентів комп'ютерної безпеки на основі керівництва NIST SP 800-61; процеси, процедури, методи управління інцидентами інформаційної безпеки захищених автоматизованих систем управління; види, класифікація, функціонування та принципи реалізації інцидентів інформаційної та кібернетичної безпеки; моніторинг загроз, захист і реагування на інциденти комп'ютерної безпеки в ICS; регламент інформування персоналу автоматизованої системи про виявлені інциденти; регламент усунення й обліку виявлених інцидентів; методи розслідування інцидентів у комп'ютерних системах; основи комп'ютерної криміналістики; моніторинг активів та мережевої безпеки, правила розмежовування доступу; моніторинг мережевої безпеки ICS; етапи розслідування інцидентів у комп'ютерних системах, придбання цифрових доказів (артефактів); методологія аналізу векторів атаки й цифрових доказів у ході вивчення та розслідування інцидентів комп'ютерної безпеки; стратегія стримування інцидента комп'ютерної безпеки, усунення наслідків, відновлення й удосконалення системи захисту та менеджменту.

Методичні рекомендації до виконання задач кейсів модельних ситуацій: із моніторингу інцидентів інформаційної та кібернетичної безпеки; використання прикладного програмного забезпечення для виявлення та дослідження інцидентів у комп'ютерних системах і мережах; класифікація та визначення принципів функціонування та принципів реалізації інцидентів інформаційної та кібернетичної безпеки; оцінка наслідків виявлених інцидентів; визначення джерел і причини виникнення інцидентів; організація і проведення розслідування інцидентів інформаційної безпеки та виявлених порушень заходів захисту інформації; прогнозування можливих шляхів розвитку дій порушників інформаційної безпеки; визначення й обґрунтування активів, ресурсів, ролі, діяльності для процесів і процедур управління інцидентами інформаційної безпеки захищених автоматизованих систем управління та організації; застосовування програмних засобів резервування й відновлення інформації в автоматизованих системах; створення альтернативних місць зберігання і обробки інформації на випадок виникнення позаштатних ситуацій; ефективної роботи з основним та допоміжним програмним забезпеченням; визначення

оптимальних програмних засобів для оперативного реагування та якісного управління інцидентами інформаційної безпеки; визначення необхідних правил і процедур виявлення інцидентів та процедур реагування на інциденти; виявлення й ідентифікація інцидентів у процесі експлуатації автоматизованої системи; усунення інцидентів, що виникли в процесі експлуатації автоматизованої системи; резервування програмного забезпечення, технічних засобів, каналів передачі даних автоматизованої системи управління.

Розроблено навчально-інформаційну платформу для віддаленого доступу проведення семінарських занять у режимі вебінарів, онлайн-конференцій за розділами: понятєвий апарат управління комп'ютерними інцидентами; аналіз основних положень стандартів ISO/AEC 27 серії з управління комп'ютерними інцидентами (ISO/IEC 27001:2005; ISO/IEC 20000:2005; ISO/IEC TR 18044:2004); реагування на інциденти комп'ютерної безпеки на основі рекомендацій NIST SP 800-61 та національних стандартів; реагування на інциденти комп'ютерної безпеки на основі рекомендацій NIST SP 800-61 та національних стандартів; аналіз потенційного ландшафту загроз, виявлення та зменшення впливу інцидентів комп'ютерної безпеки; етапи проведення аудиту мережевої безпеки, моніторинг активів; призначення й функціональні можливості інструментів Wireshark, TCPdump, Cyber Lens, ELSA, Bro та Snort; групи реагування на інциденти комп'ютерної безпеки, структури; аналіз векторів атаки.

До складу навчально-методичного комплексу входять розроблені методичні рекомендації до виконання самостійних робіт за розділами: термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99; аналіз системи управління інцидентами інформаційної безпеки NAU-CERT; інформація управління інцидентами безпеки – Ч.1, принципи управління інцидентами; «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» НД ТЗІ 2.5-004-99», ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій»; ISO/IEC 27033-1, ISO/IEC 27033-2, ISO/IEC 27033-3 «Мережева безпека»; аналіз функціональних можливостей мережевих аналізаторів; аналіз сучасних програмних продуктів систем моніторингу мережевої безпеки ICS/SCADA; принципи роботи сучасних програмних продуктів систем моніторингу середовища та виявлення аномалій; аналіз розвитку сучасних систем виявлення вторгнень; ISO/IEC 27033 «Керівництво по ідентифікації, збору,

придбанню і збереженню цифрових доказів»; огляд сучасних методик аналізу шкідливих програмних засобів.

Окремим контентом навчально методичного комплексу розроблено методичні рекомендації до виконання лабораторних робіт із можливістю дистанційного доступу для підготовки. Методичні розробки до виконання лабораторних робіт включають рекомендації: використання інструментів Wireshark, TCPdump, CyberLens, ELSA, Bro, Snort та ін., для збору даних про мережу, виявлення й аналізу загроз; здійснення моніторингу мережевого середовища та виявлення аномалій; системи виявлення інцидентів комп'ютерної безпеки; збір цифрових доказів про інцидент комп'ютерної безпеки; дослідження, класифікація та використання програмних засобів; використання YARA правил.

У процесі проєктування, розробки й упровадження НМК в освітній процес використано методи навчання: індуктивний, дедуктивний, продуктивний та метод стимулювання; інтерактивні методи: проблемної дискусії; мозкового штурму; проєктування: моделювання; дерева рішень; експертних груп, case-study.

Індуктивний метод полягає в тому, що викладач насамперед викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім, роблячи висновки, поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний із опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, застосування наукових і практичних знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією.

Інтерактивні методи: проблемної дискусії; мозкового штурму; проєктування: моделювання; дерева рішень; експертних груп застосовано у процесі лекційного курсу та семінарських занять, метод case-study застосовано у процесі підготовки до модульних контрольних робіт на платформі для дистанційного доступу.

Розроблено тестові пакети для проведення модульних контрольних робіт та підсумкового модульного контролю.

Висновки та перспективи подальших наукових розвідок. За результатами системного аналізу досягнень у галузі інформаційної безпеки здійснено обґрунтування, проєктування й розробку навчально-

методичного комплексу для забезпечення якісного освітнього процесу формування професійної компетентності з управління інцидентами інформаційної та кібернетичної безпеки.

Навчально-методичний комплекс «Управління інцидентами інформаційної і кібернетичної безпеки» включає теоретичну частину, авторську розробку навчально-методичного комплексу – інформаційний контент лекційних занять. Для педагогічного супроводу формування компетентності управління інцидентами, як складові НМК, розроблено методичні рекомендації до виконання задач кейсів модельних ситуацій: із моніторингу інцидентів інформаційної та кібернетичної безпеки інформаційної і кібернетичної безпеки; навчально-інформаційну платформу для віддаленого доступу проведення семінарських занять у режимі вебінарів, онлайн-конференції за розділами навчального модулю; методичні рекомендації до виконання лабораторних робіт, самостійних робіт та виконання індивідуальних творчих завдань, проєктування, моделювання тощо.

Для досягнення ефективності подальшого впровадження НМК в освітній процес перспективами подальших наукових розвідок є розробка диференційної рівневої шкали оцінки навчальних досягнень слухачів та здійснення моніторингу якості процесу формування компетентності управління інцидентами інформаційної та кібернетичної безпеки.

ЛІТЕРАТУРА

Гладиш, С. В. (2008). Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. *Реєстрація, зберігання і оброб. даних, Т. 10, № 1,* 116-124 (Hladysh, S. V. (2008). Support for decision-making on information security incident management in organizational and technical systems. *Registration, storage and processing, Vol. 10, no 1,* 116-124).

Гладиш, С. В., Кононович, В. Г., Тардаскін, М. Ф. (2007). Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 15,* 31-39 (Hladysh, S. V., Kononovych, V. H., Tardaskin, M. F. (2007). Comparative analysis of ISO/IEC standards and the Ukrainian regulatory framework in terms of information security incident management. *Legal, regulatory and metrological support of the information protection system in Ukraine, 15,* 31-39).

Гладиш, С. В. (2008). Реагування та обробка інцидентів інформаційної безпеки в мережі GSM. *Вісник Державного університету інформаційно-комунікаційних технологій, 1,* 58-72 (Hladysh, S. V. (2008). Response and processing of information security incidents in the GSM network. *Bulletin of*

the State University of Information and Communication Technologies, 1, 58-72).

Гнатюк, С. О. Хохлачова, Ю. Є., Охріменко, А. О., Гребенькова, А. К. (2012). Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки. *Науково-практичний журнал «Захист інформації», Том 14, № 1 (54).* URL: http://jrnl.nau. edu.ua/index.php/ZI/issue/ view/58/showToc (Hnatiuk, S. O., Khokhlachova, Yu. Ye., Okhrimenko, A. A., Hrebenkova, A. K. (2012). Theoretical foundations of construction and operation of information security incident management systems. *Scientific and practical journal "Information Security", Vol. 14, № 1 (54).* Retrieved from: http: //jrnl.nau. edu.ua/index.php/ZI/issue/ view / 58 / showToc).

Копитін, Ю. (2010). Розслідування інцидентів інформаційної безпеки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, Вип. 1 (20),* 58-65 (Kopytin, Yu. (2010). Investigation of information security incidents. *Legal, normative and metrological support of the information protection system in Ukraine, Vol. 1 (20),* 58-65).

Мужанова, Т. М. Геопросторовий підхід до забезпечення кібербезпеки. *Сучасний захист інформації, 2,* 27-31 (Muzhanova, T. M. Geospatial approach to cybersecurity. *Modern information protection, 2,* 27-31).

Стефурак, О. Р., Тихонов, Ю. О., Лаптєв, О. А., Зозуля, С. А. (2020). Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. *Сучасний захист інформації, 2,* 19-26 (Stefurak, O. R., Tykhonov, Yu. O., Laptiev, O. A., Zozulia, S. A. (2020). Improving the stochastic model to identify threats of damage or unauthorized leakage. *Modern information protection, 2,* 19-26).

ISO/IEC 27001:2005. *Information Technology. Security Techniques. Information Security Management Systems. Requirements.*

ISO/IEC 20000:2005. *Information Technology. Service Management. Part 2: Code of Practice*.

ISO/IEC TR 18044:2004. *Information Technology. Security Techniques. Information Security Incident Management*.

РЕЗЮМЕ

Воскобойников Сергей, Решетников Олег. Проектирование образовательного процесса профессиональной подготовки специалистов к управления инцидентами информационной и кибербезопасности.

В статье осуществлен теоретический анализ, обобщены результаты исследования проблемы организации подготовки специалистов по управлению инцидентами информационной и кибербезопасности. Для обеспечения качественного образовательного процесса формирования профессиональной компетентности по управлению инцидентами информационной и кибернетической безопасности осуществлены обоснование, проектирование и разработка учебно-методического комплекса «Управление инцидентами информационной и кибернетической безопасности». Для педагогического сопровождения формирования компетентности управления инцидентами,

как составляющие УМК, разработаны методические рекомендации к выполнению задач кейсов модельных ситуаций: по мониторингу инцидентов информационной и кибернетической безопасности; учебно-информационная платформа для удаленного доступа для проведения семинарских занятий в режиме вебинаров, онлайн-конференций по разделам учебного модуля; методические рекомендации к выполнению лабораторных и самостоятельных работ и индивидуальных творческих задач, проектированию, моделированию и др.

Ключевые слова: *информационная безопасность, кибербезопасность, образовательный процесс, формирование компетентности управления инцидентами информационной и кибернетической безопасности, учебно-методический комплекс.*

SUMMARY

Voskoboinikov Serhii, Reshetnilov Oleh. Design of the educational process of professional training of future specialists of information and cyber security incident management.

The article provides a theoretical analysis, summarizes the results of a study of the problem of organizing the training of information and cyber security incident management specialists. It is determined that for high-quality professional training of future specialists it is important to consider all the provisions and their study and analysis in the design of educational and methodological support of the process of forming information and cyber security incident management competence.

Based on the results of a systematic analysis of achievements in the field of information security, substantiation, design and development of an educational and methodological complex to ensure a quality educational process of professional competence in information and cyber security incident management.

The basic was the integrated application of systems, competence and activity approaches, the use of general scientific and special methods: systematic analysis and synthesis, terminological analysis, generalization. In the course of design, development and implementation of EMC in the educational process, teaching methods were used: inductive, deductive, productive and stimulation method; interactive methods: problem discussion; brainstorming; design: modeling; decision trees; expert groups, case-study.

The educational and methodological complex "Information and Cyber Security Incident Management" includes a theoretical part, the author's development – information content of lectures. For pedagogical support of forming the incident management competence, as components of EMC, methodological recommendations were developed: on monitoring of incidents of information and cyber security; training and information platform for remote access to seminars and webinars, online conferences by sections of the training module; methodological recommendations for laboratory work, independent work and individual creative tasks, design, modeling, etc.

Key words: *information security, cybersecurity, educational process, formation of information and cyber security incident management competence, educational and methodological complex.*