УДК 004.415.2
DOI https://doi.org/10.32782/2663-5941/2023.5/42

Чумаченко С.М.
ГО Асоціація фахівців цивільного захисту

Попель В.А.
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації

СИСТЕМНИЙ ПІДХІД ДО АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КОМПЕТЕНТНОСТІ ПЕРСОНАЛУ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СИЛ ОБОРОНИ УКРАЇНИ

Публікація присвячена проблемам автоматизації системи підбору та оцінки відповідності персоналу, що має забезпечувати безпеку об'єктів критичної інфраструктури Сил оборони України. В статті розглянуто основні нормативні документи, вимоги до персоналу та шляхи оцінки відповідності його знань, умінь і компетенції. Враховані вимоги професійних стандартів, розроблених для сфери критичної інфраструктури Сил оборони України та захисту інформації. Ця робота має на меті визначити базові проблеми, пов'язані з підбором кваліфікованого персоналу, оцінки його відповідності та визначення якості роботи в процесах діяльності. Матеріали статті стосуються саме об'єктів критичної інфраструктури Сил оборони України і розглядають особливості, пов'язані з процесами забезпечення безпеки критичної інфраструктури. Результати, отримані в результаті проведеного аналізу проблем персоналу в сфері забезпечення безпеки об'єктів критичної інфраструктури, мають допомогти керівникам установ, організацій, підприємств а також підрозділам HR при формуванні та комплектуванні підрозділів, підготовці та розстановці кадрів. При підготовці публікації розглянуті основні нормативні акти, що регулюють процеси захисту критичної інфраструктури, досвід розвинутих країн, в першу чергу США та Європейського Союзу, стандарти безпеки (ДСТУ ISO/EN 27001, NIST Special Publication 800-181) та рекомендовані практики.

Висновки містять рекомендації щодо автоматизації системи підбору, підготовки та підвищення кваліфікації персоналу в сфері захисту об'єктів критичної інфраструктури, а також її інформаційної та кібербезпеки. Висновки публікації містять рекомендації щодо удосконалення автоматизації процедур підбору та розстановки кадрів, планування підвищення кваліфікації та створення системи професійної підготовки, що базується на системі управління знаннями.

Ключові слова: *автоматизація, системи управління, захист критичної інфраструктури, компетентність персоналу, стандарти інформаційної безпеки, знання, навички, компетенції, управління знаннями.*

Постановка проблеми. В умовах російської військової агресії до першочергових завдань держави належить забезпечення захисту критичної інфраструктури (КІ) Сил оборони України. Основні засади та принципи захисту КІ визначені Законом України «Про критичну інфраструктуру» [1]. В контексті практичної організації захисту Закон передбачає впровадження автоматизованої системи безпеки КІ Сил оборони України. Її побудова і забезпечення належного рівня захисту стикається з проблемами, що мають безпосередній вплив як на стан безпеки системи, так і на потреби в ресурсах, в тому числі фінансових, що вимагаються для їх вирішення. Однією з найбільш нагальних і ключових в цьому сенсі є проблема компетентності персоналу, що забезпечує захист і відновлення об'єктів інфраструктури. Саме від рівня компетентності та кваліфікації персоналу залежить як обсяг ресурсів, так і час реагування на інциденти безпеки, що безпосередньо впливає як на обороноздатність країни, так і на якість життя населення.

Захист об'єктів КІ є життєво важливим завданням в умовах військової агресії для Сил оборони України (СОУ). Виняткова потреба в організації захисту критичної інфраструктури знайшла відображення в законодавстві [1, 2, 3]. На даний момент визначено ознаки об'єктів критичної інфраструктури (ОКІ), порядок їх ідентифікації, обліку, об'єднання в сектори управління, встановлений порядок управління кожним сектором, в тому числі в контексті організації захисту визначених об'єктів.

Враховуючи встановлене законом організаційне об'єднання ОКІ СОУ в складну ієрархічну

структуру, яка має призначений державою уповноважений орган у сфері захисту критичної інфраструктури [1], розглянемо актуальні аспекти автоматизації системи підготовки та підвищення компетентності персоналу, задіяного в забезпеченні захисту як окремих ОКІ, так і всієї СКІ в цілому.

Аналіз останніх досліджень і публікацій. Система кадрового менеджменту, на думку класиків цього напрямку досліджень, діяльності та використання (Армстронг, Барнард, Друкер, Карлоф, Маслоу, Мескон, Тейлор, Фоллет, Файоль та ін.), складається з наступних тісно пов'язаних та залежних один від одного елементів технологій (рис. 1):

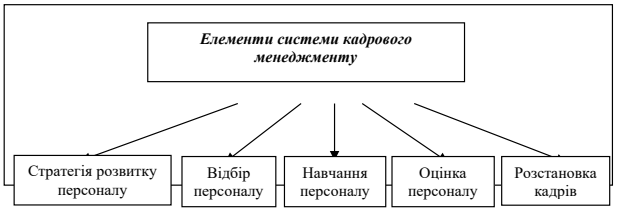

Рис. 1. Складові системи кадрового менеджменту

При цьому, категорично відокремити один від одного елементи системи кадрового менеджменту неможливо. Вони складають єдине ціле, оскільки неможливо здійснити відбір, навчання та розстановку кадрів без оцінювання персоналу; навчання персоналу без відбору та оцінювання; розстановку кадрів без відбору персоналу, його оцінювання та навчання. Тому головною технологією кадрового менеджменту є оцінка персоналу, яка визначає його якість, його придатність до виконання відповідних обов'язків та завдань щодо захисту КІ СОУ.

Поняття «людиноцентризму» знайшло своє відображення спочатку у філософській науці, а пізніше з розвитком системи управління людськими ресурсами було розповсюджено й у кадровому менеджменті.

Як відмічав Президент Академії педагогічних наук України академік В.Г. Кремень, «…філософія людиноцентризму – не лише чергове філософське і антропологічне вчення, а перетворення філософствування з гуманістичних міркувань як таких, в новий тип метафілософії і світогляди, що безпосередньо стосуються вищих сенсів буття, які діють через життя і живе мислення. Звертаючись до проблем духовності, моральності та єдності внутрішнього світу людини, людиноцентризм, як принцип цілісного розуміння особи, відповідає пошукам сучасної соціально-філософської думки.

Людиноцентризм відповідає вимогам і запитам сучасної постіндустріальної цивілізації, яка шукає людину досвідчену, творчу, ініціативну і у той же час інноваційно мислячу».

Принцип людиноцентричності вже багато років поставлено у центрі діяльності органів управління персоналом, служб персоналу, кадрових органів армій провідних держав світу.

Якісний відбір персоналу СКІ СОУ повинен вирішуватися за допомогою методів, які дають змогу визначити ступінь придатності того чи іншого громадянина до виконання обов'язків професійної діяльності або ступеню його придатності до нової для нього посади. Визначення ступеню придатності (умовної придатності, непридатності) людини (особи) до виконання військово-професійних обов'язків можливе лише при використанні технологій професійного психологічного відбору на військову службу, на нову посаду [4].

Аналіз професійної діяльності здійснюється в рамках професіографії, на підставі професіографічних досліджень, вивчення змісту кожної окремої посади (спеціальності) [11].

Стратегічні підходи до використання технологій кадрового менеджменту у напрямках управління персоналом, управління кар'єрою у військових організаціях держав-членів НАТО використовуються ще з початку XX сторіччя.

Система просування по службі в арміях НАТО відпрацьована багатьма роками застосування та відповідною нормативно-правовою базою: у США (1947, 1981), ФРН (1971), Франції (1976), Іспанії (1999), Угорщина (2002) [6-9].

Вся система просування офіцерів Збройних Сил (ЗС) США по службі побудована на культивуванні духу змагання за принципом: чим вище військове звання і посада, тим більш жорсткими повинні бути критерії відбору [9]. Вона, в основному, забезпечує справедливу селекцію в офіцерському корпусі. Суворо дотримуються терміни вислуги в кожному військовому званні. Вважається, що офіцер не може «засиджуватись», не просуваючись службовими сходами, і якщо встановлені терміни перевищені, він повинен бути звільнений у відставку як безперспективний. Так, наприклад, вчинять з капітаном, який має вислугу більше 16 років (4+два капітанські строки по 6 років), або полковником з 30-річною вислугою (25+5 років максимального полковничого строку), які не мають перспектив подальшого просування по службі. Для отримання чергового військового звання офіцерами у всіх видах ЗС США встановлені єдині мінімальні терміни військової служби (вислуги): для отримання звання 1-го лейте-

нанта – 2 роки, капітана – 4, майора – 10 років, підполковника – 15 років, полковника – 22 роки.

Формуванню якісного та професійного управлінського складу присвячено багато робіт вітчизняних науковців: Г. Атаманчук, Н. Нижник, А. Оболонський, В. Олуйко, Є. Охотський, І. Сурай, О. Турчинов та ін. [10]. Перший поштовх та найбільший вплив на розвиток напрямку створення та забезпечення рівня професіоналізму ланок управління СКІ сприяли роботи класиків менеджменту загалом та кадрового менеджменту зокрема. Класиками даного напрямку є М. Армстронг, М. Вебер, А. Маслоу, С. Тейлор, Є. Мескон, П. Друкер та ін.

Під час досліджень у цьому напрямку були створені перші стандарти професійної служби, які базувалися на «системі заслуг і достоїнств», що, в свою чергу, вимагало визначення та затвердження обліку потрібних ділових та особистісних якостей при призначенні та просуванні на посадах управлінської ланки будь-якого рівня СКІ, незалежно від раси, кольору шкіри, релігії, статі, сімейного стану, віку. Головними критеріями вважалися найбільша компетентність, високі моральні та етичні стандарти.

Служби персоналу держав членів НАТО визначають, що вибір кандидата на посаду СКІ СОУ повинен бути:

– об'єктивним і базуватися на оцінюванні заслуг (досягнень) кожного кандидата;

– конкурентним, але здійснюватися за процесами та показниками, які повинні бути зрозумілими для будь-якого військовослужбовця – солдата, сержанта або офіцера;

– оцінювання кандидата є ключовою частиною відбору як для членів відбіркових комісій, так і для офіцерів, які здійснюють первинний відбір кандидатів у частинах (з'єднаннях);

– відбір повинен враховувати питання щодо індивідуальних, особистісних переваг кандидата для характеру типу діяльності призначення, присвоєння військового звання, направлення на навчання і підготовку [10–12].

Метою статті є наукове обґрунтування застосування сучасних інформаційних технологій автоматизації системи підготовки персоналу для захисту ОКІ СОУ, як невід'ємного органічного доповнення базового інструментарію системи автоматизованого управління безпекою ОКІ.

Виклад основного матеріалу. Вимоги до організаційного забезпечення ОКІ визначені, в тому числі, Постановою КМУ від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [3, с. 2]. Вимоги передбачають як створення відповідних підрозділів, так і включення до них фахівців, що мають виконати дії щодо забезпечення безпеки ОКІ СОУ. В той же час, на рівні самого об'єкту, досить складно знайти як необхідний персонал, так і визначити ступінь його відповідності та готовності виконання відповідних посадових обов'язків.

При проведенні роботи з підбору та підготовки персоналу важливо чітко розуміти, якими саме знаннями, навичками і компетенціями має володіти фахівець. Зміст такої підготовки витікає з концепції захисту КІ, яка в значній мірі запозичена з досвіду розвинутих країн, що пройшли значний шлях у створенні системи захисту КІ і мають сталий досвід. Загальним підходом в організації захисту ОКІ є те, що захист СКІ базується на системі управління, і, відповідно, на інформаційній інфраструктурі, як основі функціонування будь-якої системи менеджменту. Тому головна практика захисту будується на стандарті ДСТУ ISO/EN 27001 [14], який визначає вимоги до системи управління інформаційної безпеки. Цей стандарт орієнтується, в свою чергу, на ДСТУ ISO/EN 9001, і є по суті системою якості, впровадження якої дозволяє забезпечити захист інформації в організації. Згідно з концепцією стандарту, захисту підлягає та інформація, що визначена організацією, як цінна, а також та, необхідність захисту якої визначено законом. Таким чином, вимоги стандарту, стосуючись інформації, чіпляють всі бізнес-процеси і аспекти діяльності організації, управління організацією, внутрішні та зовнішні взаємодії, технології та персонал. Вимоги до персоналу визначаються в розділі 7 стандарту, і визначають відповідальність організації за забезпечення того, щоб персонал був компетентний, мав відповідну освіту, підготовку або досвід.

У [14] наведено порівняльний аналіз з нормативами і методами в роботі з персоналом в сфері безпеки КІ інших країн, розглянуті кращі практики. Враховані вимоги стандартів, в тому числі ДСТУ ISO/EN 27001 «Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги», NIST Special Publication 800-181 «Workforce Framework for Cybersecurity (NICE Framework)» [15].

Зокрема, можливо виділити деякі важливі компетенції, знання та навички:

– персонал повинен бути компетентним у виявленні потенційних загроз КІ та вміти запобігати їм. Це може включати в себе вивчення методів

кіберзахисту, фізичної безпеки та інших аспектів безпеки ОКІ СОУ;

– персонал має бути навчений реагувати на різноманітні інциденти, такі як природні катастрофи, техногенні аварії або кібератаки. Важливо вміти швидко та ефективно реагувати на небезпеку та забезпечити безпеку персоналу і ОКІ СОУ;

– компетентний персонал має знати, як забезпечувати безперебійну роботу ОКІ СОУ в умовах кризи або інциденту. Це може включати в себе роботу з резервними джерелами живлення, водопостачанням, системами охорони, інформаційними технологіями тощо;

– персонал має розуміти закони та нормативні документи, що стосуються безпеки ОКІ СОУ і дотримуватися їх. Невиконання правових вимог може призвести до серйозних юридичних наслідків;

– загрози та технології постійно змінюються, тому персонал має бути готовий до навчання та постійного оновлення своїх знань і навичок, як у сфері безпеки, так і в сфері іншого функціоналу.

Усі ці аспекти, вимоги, напрямки компетентності спрямовані на формування здатності персоналу забезпечити надійну і безпечну роботу ОКІ СОУ та захистити їх від можливих загроз.

Належна підготовка персоналу, що має забезпечити захист критичної інфраструктури, вимагає створення відповідної концепції. Така концепція має забезпечити певну уніфікацію, зокрема, в частині предметної області – забезпечення безпеки ОКІ СОУ, в частині вимог до фахівця – застосування професійних стандартів, в частині процедури – застосувати типові методики та процедури на рівні корпорації – СКІ.

Для застосування найкращих практик в сфері захисту СКІ необхідно враховувати складність проблеми, вимоги до застосовності, гнучкості та рівня узагальнення методик, обмеження в ресурсах, особливо – в часі. В найбільшій мірі, при формуванні системи роботи з персоналом, задачі організації захисту КІ відповідає концепція керування знаннями [17, с. 1–3], оскільки вона має можливість компенсувати ресурсні обмеження більш активним застосуванням інтелектуальної складової. Ця концепція будується на визначенні знань, як цінності і активу, а також врахування в цьому активі практичних навичок, уміння тощо, що мають окремі фахівці ОКІ СОУ. Згідно концепції, знання є важливим елементом ресурсів СКІ, і керування цим ресурсам надасть додаткові можливості при організації дій в екстремальних умовах аварій, тероризму агресора, атаках та ліквідації наслідків на ОКІ СОУ.

Застосування концепції не вимагає створення нових функцій або внесення змін в бізнес процеси. Вбачається, що ця концепція діє на рівні розуміння керівниками (менеджерами) організації головних принципів концепції і застосування цих принципів при проведенні звичної діяльності. До таких можливо віднести:

1. Створення бази знань. Процедура створення знань в значній мірі базується на ідентифікації знань, виділення корисних знань, створення бази знань і доведення цих знань до членів колективу, яких саме ці знання стосуються. Для цього може проводитися пошук і впровадження процесів, які сприяють створенню нових знань. Це може включати в себе стимулювання робочих груп для обміну ідеями, проведення брифінгів та тренінгів для створення бази знань.

2. Ідентифікація та документування знань. Для того, аби забезпечити можливість врахування знань, застосування і керування ними, необхідно визначити знання, по можливості задокументувати – описати, внести до бази знань і пов'язати з процесами та фахівцями. Доцільно долучити до цього процесу весь колектив ОКІ СОУ. Для забезпечення мотивації з боку фахівців доцільно ввести заохочення співробітників ділитися своїми знаннями та досвідом. Документування знань є важливим елементом концепції, оскільки не закріплені у вигляді документів знання легко втрачаються. З метою документування можуть бути застосовані різні інструменти, інструкції, процедури бази знань. В існуючому варіанті це може бути ведення бази даних або внутрішнього порталу для зберігання і поширення інформації для ОКІ СОУ.

3. Поширення і передача знань. Організація має розробити автоматизовану систему навчання, яка враховує і застосовує принципи концепції управління знаннями. Така система може включати створення програми навчання та розвитку, що допомагає співробітникам набувати нові знання та навички, передбачити використання ефективних методів навчання, таких як тренінги, вебсемінари, онлайн-курси і менторство.

4. Знання, як цінний актив, мають бути доступні для тих членів колективу ОКІ СОУ, якими вони можуть бути використані. Для цього необхідних спільний доступ до інформації. Цей доступ може бути організований шляхом створення централізованих інформаційних систем для доступу до інформації та обміну нею між співробітниками, використання захищених мереж або спеціального програмного забезпечення для спільного доступу до ресурсів.

5. Ключовим елементом впровадження концепції управління знаннями є забезпечення мотивації до спільного навчання. Мотивом може бути як матеріальне, так і моральне заохочення, правильно побудована кар'єрна модель, участь в результатах діяльності СКІ. Має бути забезпечено створення мотиваційних систем та нагород для тих, хто активно ділиться знаннями та навчає інших, заохочення колективного навчання та обміну досвідом.

6. Знання, як цінний актив, мають бути захищені. Захист знань може бути забезпечений шляхом впровадження конфіденційності та захисту цінної інформації, розробки політик щодо обмеження доступу до деяких видів знань, запровадження в організації відношень, що включають елемент захисту знань в корпоративній культурі ОКІ.

7. Управління знаннями, як процес, потребує контролю та аналізу. З цією метою можливо запровадити моніторинг і оцінку результатів управління базою знань, включаючи вимірювання впливу здійснених заходів на продуктивність та результати ОКІ СОУ.

8. Культура відношень в колективі ОКІ СОУ (корпоративна культура), є елементом автоматизованої системи управління (включно управління базою знань) і в значній мірі результатом впровадження концепції управління знаннями. Корпоративна культура посилить потенціал організації, якщо буде базуватися на відкритості та співпраці. Менеджмент ОКІ СОУ має стимулювати поширення культури, в якій співробітники відчувають, що їхні думки та ідеї важливі і їхній внесок оцінюється. Завдяки цьому відбувається створення сприятливого середовища для обміну ідеями та вільної комунікації.

Управління знаннями в сфері інформаційної безпеки і захисту КІ може стикатися з рядом проблем і викликів. До таких належить швидка зміна технологій і загроз, оскільки сфера безпеки постійно еволюціонує, і нові технології та загрози ОКІ СОУ з'являються дуже швидко. Це ускладнює постійне оновлення знань персоналу та навчання їх новим методам інформаційного захисту, але при цьому підвищує важливість самої задачі безпеки ОКІ СОУ. Деякі члени персоналу можуть не розуміти повністю загрози безпеки або не вважати їх серйозними. Така ситуація може призвести до недостатнього дотримання політик безпеки та правил користування інформацією.

Недостатнє фінансування для навчання та розвитку персоналу у сфері безпеки ОКІ СОУ призводить до систематичного обмеження доступу до ресурсів та навчальних програм. Недостатнє спілкування, недостатній обмін інформацією та знаннями між різними частинами організації може спричинити недооцінку загроз та втрату можливостей для вчасного реагування на інциденти ОКІ СОУ. Відсутність чітких та ефективних процесів автоматизованого управління базою знань може призвести до плутанини та втрат часу. Різні ОКІ СОУ мають різні корпоративні культури та структури, в організаціях з вищим рівнем ієрархії, як правило складніше реалізувати ініціативи з управління базою знань, які потребують відкритого обміну інформацією. В таблиці 1 наведені приклади застосування концепції управління знаннями на рівні стратегії розвитку організації:

Провідні міжнародні компанії активно впроваджують стратегії управління знаннями, щоб підвищити ефективність, сприяти інноваціям, зміцнити комунікації та поліпшити процеси прийняття рішень. У кожному випадку стратегії адаптуються під конкретні бізнес-процеси та корпоративну культуру компанії, що забезпечує максимальну користь від їх впровадження.

З аналізу матеріалів таблиці 1 випливає, що управління знаннями – це процес створення, розповсюдження, використання та зберігання знань у організації з метою підвищення її спроможності в усіх аспектах діяльності. Дані аналізу свідчить, що сучасні системи управління знаннями, як правило, базуються на застосуванні автоматизованих інформаційних систем, які інтегровані в бізнес процеси організації. Успішне впровадження стратегії управління знаннями в організації вимагає системного підходу, підтримки керівництва та активної участі всіх співробітників. Правильно обрана і реалізована стратегія управління знаннями є потужним інструментом для підвищення ефективності та досягнення стратегічної мети ОКІ СОУ.

Має бути впроваджена системи моніторингу та оцінки відповідності для всіх ОКІ в системі. Мають також бути розроблені методичні і навчальні матеріали, а також впроваджені заходи сприяння за яких виникне і зможе стало функціонувати система навчання, яка забезпечить підготовку різних фахівців в єдиній парадигмі СКІ.

Сукупність цих заходів формує систему підготовки кадрів загалом для системи захисту КІ. На даний момент до найбільш розвинутих систем захисту критичної інфраструктури належить система, яка успішно функціонує в США. З її детальним описом можливо ознайомитись в документі «Національний план захисту інфраструктури

Таблиця 1

Застосування системи управління знаннями в організації

№	Компанія	Впроваджена система управління знаннями (СУЗ)	Результати впровадження
1.	Microsoft	власні рішення для управління знаннями, такі як SharePoint та Microsoft Teams	Ці інструменти допомагають командам спільно працювати над проектами, ділитися знаннями та документацією, що підвищує продуктивність роботи
2.	Siemens	впроваджено систему управління знаннями, яка охоплює обмін знаннями, навчання співробітників та співпрацю між різними відділеннями	Організація підвищила інноваційність та забезпечила ефективність розробки нових продуктів. Система сприяє швидкому пошуку та обміну знаннями, поліпшує комунікацію та співробітництво між відділами та різними бізнес-одиницями компанії
3.	IBM	IBM використовує розширену стратегію KM для підтримки своїх глобальних команд, включаючи форуми, віртуальні спільноти та системи електронного навчання	Це дозволяє компанії швидко адаптуватися до змін ринку, ефективно управляти проектами та підвищувати кваліфікацію співробітників
4.	Daimler AG	розробила спеціалізовану платформу для обміну знаннями та найкращими практиками між власними інженерами та сторонніми розробниками	забезпечено більш ефективне використання інноваційних технологій та рішень в різних проектах та продуктах компанії
5.	Novo Nordisk (Данія)	Novo Nordisk активно інвестирує у програми навчання та розвитку для своїх співробітників, в тому числі у внутрішні академії та тренінгові центри	відбувається підвищення кваліфікації та розвиток навичок співробітників, що позитивно впливає на продуктивність та інноваційність компанії
6.	Santander Bank (Іспанія)	банк використовує інструменти аналітики та інтелектуального аналізу даних для кращого збору та обробки інформації про клієнтів, продукти та ринкові тренди	підвищення ефективності в прийнятті рішень, підвищення якості обслуговування клієнтів та оптимізація внутрішніх процесів банку
7.	ABB (Швейцарія)	ABB впроваджує рішення з управління знаннями для інтеграції різних баз даних, систем проектування та інженерних інструментів, щоб сприяти співпраці між фахівцями	більш ефективна координація проектів, скорочення часу на розробку нових продуктів та підвищення якості рішень

(NIPP)» [5] на сайті профільної урядової організації CISA (агентство в структурі Міністерства внутрішньої безпеки США, що відповідає за захист критичної інфраструктури). NIPP – це документ, який визначає стратегічні цілі, пріоритети та підходи до захисту критичної інфраструктури, такої як енергетичні системи, транспорт, комунікації та інші важливі сектори від різних загроз, включаючи кібератаки, природні лиха та терористичні акти. План включає опис структури управління та співробітництва між державними та приватними секторами, а також визначає методи аналізу ризиків та заходи щодо їх зниження. Він регулярно оновлюється, щоб враховувати актуальні загрози та технологічні зміни. Визначає він також і базові вимоги до персоналу, який задіяний при виконанні задач захисту критичної інфраструктури.

Перевага моделі захисту критичної інфраструктури США полягає також в тому, що до неї розроблена серія національних стандартів та рамок (NIST, FISMA та інші), які містять достатній набір вимог та практик для охоплення більшості елементів захисту КІ.

Можливо виділити такі риси цієї системи:

1. Вимоги до кваліфікації, знань та навичок фахівців базуються на стандарті NIST 800-181 «Workforce Framework for Cybersecurity (NICE Framework)» [14].

2. Визначені спеціальності, для яких відповідно до загальних вимог стандарту розробляються професійні стандарти.

3. Для спеціальностей виділені окремі функції, для яких можуть бути створені спеціалізовані навчальні курси, навчання та перевірка знань по яким реалізуються на автоматизованих навчально-тестувальних системах.

4. З метою оцінювання відповідності фахівців застосовуються центри оцінювання, при чому чинними є оцінки як держави, так і деяких недержавних центрів навчання (таких, як Cisco, Microsoft і деяких інших).

Приблизно таку саму модель на даний момент реалізує і Україна. Уповноваженим органом рекомендовані до використання стандарти NIST. На основі стандарту NICE Framework розроблено шість і готується ще п’ятнадцять професійних

стандартів. Створено та акредитовано профільний Кваліфікаційний центр, завданням якого є визначення відповідності кваліфікації вимогам професійних стандартів у сфері інформаційної безпеки. Проводяться системі заходи щодо впровадження інших важливих елементів системи підготовки та оцінювання кадрів для сфери захисту КІ. В самій системі навчання можливе застосування засобів автоматизації. Існує багато навчально-тестувальних систем для безпосереднього та дистанційного навчання. Такі системи функціонують в більшості навчальних закладів, тому наводити детальний опис прикладу немає потреби. Структурна схема опису типової навчально – тестувальної системи наведено на рис. 2.

Головним компонентом такої автоматизованої системи є навчальні курси, які вони пропонують персоналу ОКІ СОУ. Такі навчальні курси мають надавати знання та навички, що відповідають кваліфікаційним вимогам професійних стандартів. Розділення професії на модулі, кожний з яких відповідає певній виробничій функції, дозволить сформувати гнучку систему підвищення кваліфікації, яка може складати 1–2 річні плани, за якими фахівці отримають можливість без суттєвого відриву від виробництва отримати необхідні знання в повному обсязі.

Такі центри можуть мати централізовану базу знань з методичних матеріалів, накопичувати матеріали екзаменів, бути об’єднані в мережу, містити елементи моніторингу та обробляти статистику навчання, формуючи об’єктивні дані щодо стану професійної готовності персоналу всього сегменту СКІ.

Програмні засоби можуть забезпечити реалізацію сучасних підходів до навчання, включити практику на імітаційних тренажерах, забезпечити елементи системи управління знаннями.

Для поліпшення продуктивності та автоматизації кадрових процесів, перш за все пов’язаних з моніторингом та відбором, підбором і просуванням персоналу ОКІ СОУ, на них створені сотні програмно-аналітичних платформ.

Основою такого програмного забезпечення є аналітичні системи Business intelligence (BI), які визначаються як комп'ютерні методи та інструменти для організацій, що забезпечують переведення транзакційної ділової інформації

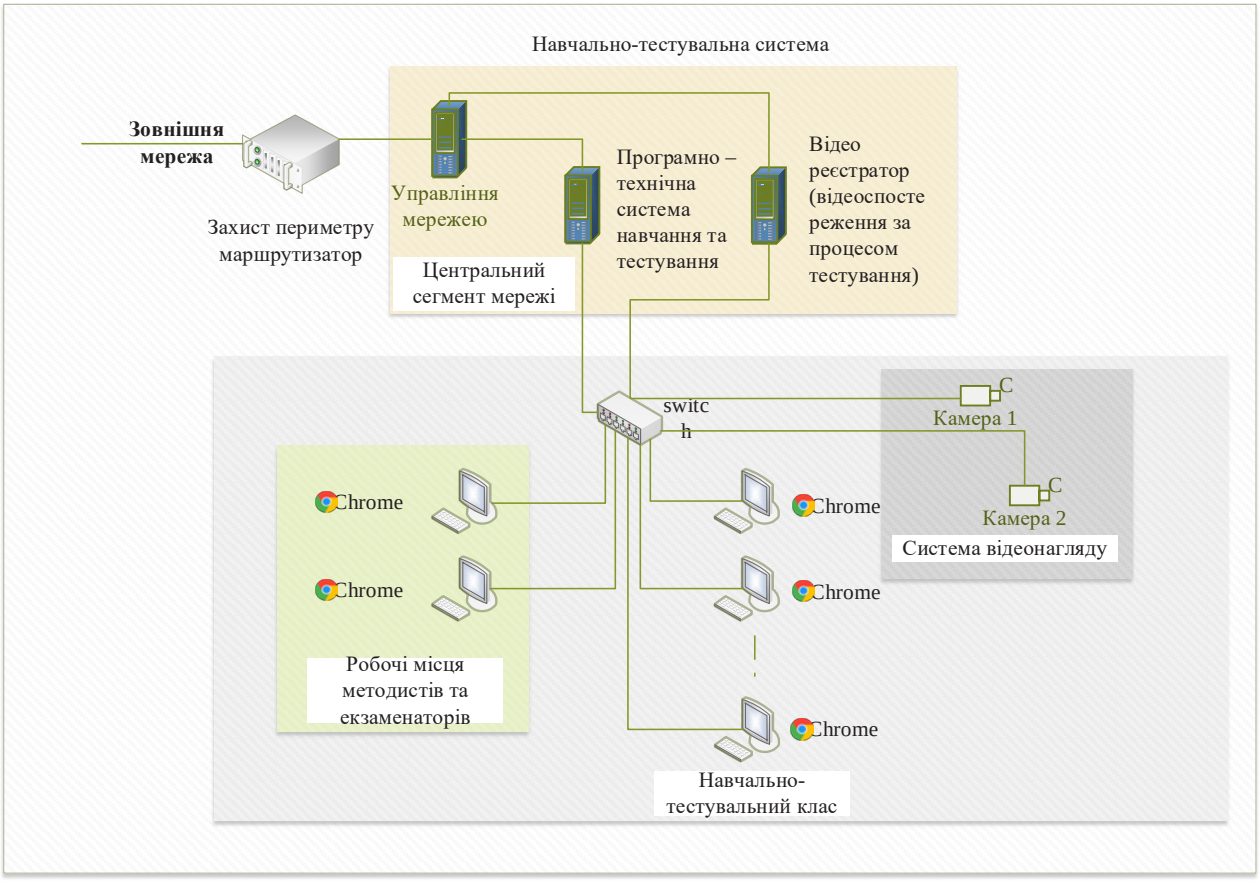

Рис. 2. Структурна схема типового навчально-тестувального центру

в доступну для користувачів форму, придатну для бізнес-аналізу, а також засобів для масової роботи з такою обробленою інформацією [18].

Лідируючі позиції з розробки програмного забезпечення у даній галузі належать відомим провідним компаніям: SAP, ORACLE, ADP, IBM. Також останнім часом у даному процесі задіяно велику кількість нових компаній.

Останніми тенденціями з розробки спеціального програмного-аналітичного забезпечення *Business intelligence* є використання у їх складі передових інформаційних технологій, заснованих на хмарних обчисленнях, що надає переваги у їх використанні на різних типах робочих станцій та мобільних пристроях.

Крім основного переліку функцій з обробки великого масиву даних (*Big Data*), деякі програмно-аналітичні додатки можуть включати наступні можливості на інновації:

1. *Тестування та оцінювання компетентності персоналу* – призначене для попередньої оцінювання знань, умінь, навичок, набутих кваліфікацій претендентів на посаду для вибору кращого з них. Найбільш затребуваним програмним забезпеченням, яке користується попитом у багатьох світових компаніях у даній сфері є програмно-аналітичні платформи та сервіси:

HackerRank – платформа оцінювання рекрутинговими організаціями компетентностей трудових ресурсів для відбору та найму працівників з необхідними якостями;

Pymetrics – сервіс, який використовує неупереджені алгоритми для пошуку підходящих кандидатів, використовуючи гейміфіковані нейробіологічні тести. Сервіс на ринку відносно недавно, але вже добре себе зарекомендував;

Self Management Group – програмно-аналітичне забезпечення для управління набором персоналу з інтегрованою діагностикою та оцінками для залучення, управління та оцінкою кандидатів.

2. *Використання штучного інтелекту*. Використання технологій штучного інтелекту (ШІ) в автоматизованих бізнес-аналітичних процесах. Найкращими сервісами серед яких є:

Ideal – використовує технології ШІ для відбору кандидатів, аналізуючи комплексну інформацію про них: резюме, оцінки та дані про їх результативність;

Textio – глобальна система з уніфікації за єдиним стандартом текстових даних опублікованих резюме кандидатів, написаних за різним поданням та структурою, та автоматичного виправлення можливих граматичних та синтаксичних помилок у тексті. Головна особливість, яку пропонує система – здатність виявляти закономірності в мові, допомагаючи кадровим органам якісніше проводити відбір кандидатів.

3. Використання *Applicant Tracking Systems (ATS)* – система відстежування кандидатів:

Bullhorn – спеціалізований аналітичний додаток, призначений для пошуку та відбору кандидатів;

SAP SuccessFactors – спеціальне програмне та інформаційно-аналітичне забезпечення для управління людськими ресурсами. Система використовує технології, засновані на методології управління талантами;

iCIMS – комплекс програмного забезпечення для оптимізації роботи кадрових менеджерів, задіяних у процесах рекрутингу персоналу, його просування та управління кар'єрою;

Oracle Taleo Cloud Service – спеціальне програмне та інформаційно-аналітичне забезпечення для пошуку, рекрутингу, просування й утримування кваліфікованих спеціалістів за допомогою багатофункціонального пакета програмного забезпечення;

Workday – програмна система, яка об'єднує бухгалтерський облік, управління персоналом і планування в єдиній хмарній ERP-системі для підвищення ефективності бізнесу;

SmartRecruiters – спеціальне програмне та інформаційно-аналітичне забезпечення, яке за рахунок використання можливостей ШІ і соціальних мереж, дозволяє кадровим менеджерам ефективними способами проводити пошук кандидатів та проводити відбір кваліфікованих спеціалістів у будь-якій частині світу.

Крім вузько направлених у сфері управління персоналом *BI*-систем, існують універсальні системи, можливості яких дозволяють проводити аналіз *Big Data* у будь-якій сфері діяльності. До найбільш потужних засобів бізнес-аналітики, за версією видання Gartner за 2020 і попередні роки, відносяться програмні продукти компаній *Tableau*, *Qlik* і *Power BI*.

Головною їх відмінністю від готових *BI*-рішень є дещо інші підходи до порядку обробки даних, а також їх пристосованість до будь-яких організаційних вимог стосовно побудови та впровадження на автоматизованих робочих місцях інформаційних панелей *(dashboard)*.

Інформаційні панелі є складовою частиною *BI*-системи, призначених для візуалізації великого масиву інформації, що аналізується у вигляді графіків, діаграм та інших форм відображення

кількісної інформації, що, в свою чергу, спрощує усвідомлення та допомагає керівництву оцінити реальний стан справ і прийняти обґрунтоване рішення.

Досить функціональним є використання технології in-memory processing (проведення аналізу та обчислень в оперативній пам'яті) та Business Discovery (модуль бізнес досліджень) у програмних продуктах *Qlik*, яка дозволяє аналізувати бізнес-інформацію на будь-якому рівні, уникаючи трудомістких і дорогих робіт з побудови сховищ і багатовимірних *OLAP*-кубів. Будь-які обчислення *BI*-системи *Qlik* виконуються миттєво навіть при дуже великих обсягах інформації при одночасній роботі великої кількості користувачів, що значно підвищує ефективність роботи. Алгоритми побудови аналітичних моделей, їх переваги та недоліки показані на рис. 3.

Асоціативна архітектура моделі дозволить управляти взаємозв'язками між даними не на прикладному рівні, а на рівні внутрішніх механізмів платформи. Програмний засіб, в якому це реалізовано, зберігає в оперативній пам'яті окремі таблиці даних і асоціативні зв'язки між ними, де кожне значення кожного поля пов'язано з усіма іншими значеннями асоціативної моделі. При створенні нових вибірок, користувач бачить: як дані пов'язані з його запитом, дані, які не входять до вибірки. Це дозволяє користувачеві працювати максимально комфортно, відповідаючи на нові питання самостійно без допомоги фахівців інформаційних технологій [10].

Сервіс *Qlik Business Discovery* дозволяє аналізувати інформацію у різних інформаційних розрізах (за часом актуалізації) і незалежно від того, в яких автоматизованих системах управління персоналом дана інформація зберігається, швидко розгортатися та масштабуватися навіть при використанні великої кількості джерел даних, має у своєму складі засоби спільної аналітики у реальному часі.

Особлива увага при побудові *BI*-систем приділяється їх реалізації. Головна ідея цього етапу полягає в тому, що реалізація системи повинна відбуватись не на заключному етапі її створення, а проводитись паралельно від самого початку створення системи. Провідними світовими компаніями розробниками програмного забезпечення рекомендовано починати розробку з простої версії, швидко її впроваджувати на практиці й поступово покращувати та поширювати автоматизовану систему на основі досвіду, одержаного при взаємодії між користувачем, системою й тим, хто її проєктує.

Отже, для багатьох організацій у світі використання *BI*-систем з обробки великих масивів даних (*Big Data*), призначених для ефективного управління персоналом, особливо націлених на пошук, відбір і утримання кваліфікованих спеціалістів, дедалі з кожним роком стає нормою, без якої неможливо вести ефективний бізнес для отримання максимальних прибутків.

Використання спеціального програмно-аналітичного забезпечення у діяльності служб персоналу ОКІ СОУ усіх рівнів управління організаційною ієрархією, дозволить вирішити низку проблемних питань, пов’язаних з прискоренням темпів професіоналізації Сил оборони України, підвищення якості укомплектованості, прозорість, об’єктивність та обґрунтованість кадрових

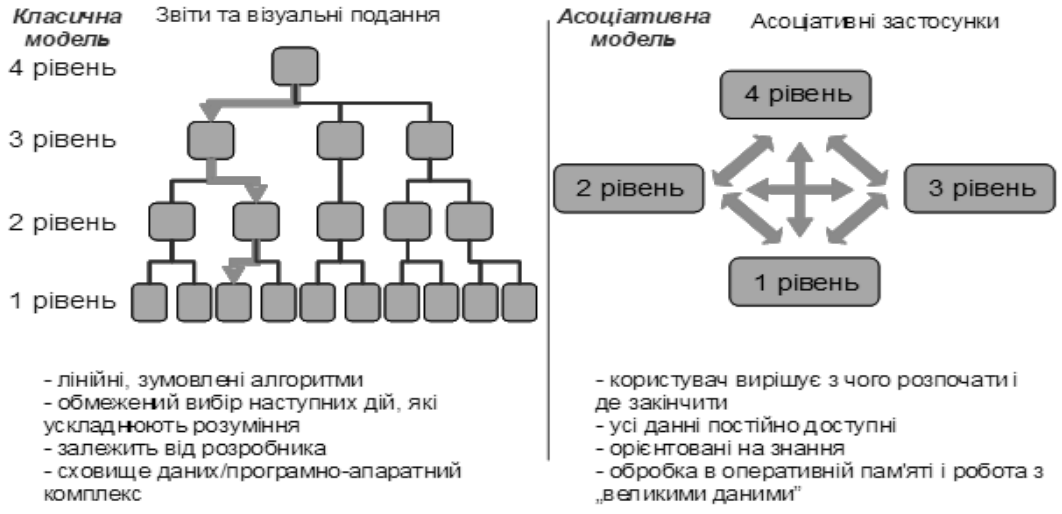

Рис. 3. Алгоритми побудови аналітичних моделей

рішень ОКІ СОУ, якісним відбором та просуванням найкращих кандидатів на ключові посади.

За результатами оцінювання та визначення необхідної кількості кандидатів до Резерву на відповідні посади складається рейтинг (за спеціальностями, спеціалізаціями, посадами, званнями). Рейтинг – список кандидатів, складений за результатами конкурсного відбору за кількісним показником набраних ними балів за принципом від більшого балу до меншого.

При складанні рейтингу необхідно враховувати:

N-ну кількість параметрів (показників, критеріїв оцінювання);

вагу кожного параметру та його можливий вплив на загальний результат;

кількість членів (кількість голосів), які приймають участь у складанні рейтингу;

вагу кожного голосу в залежності від статусу члена комісії (голова, експерт даного напрямку, фахівець вищої категорії за напрямом діяльності, начальник, колега, підлеглий).

За теорією, рейтинг – нижня межа довірчого інтервалу Вільсона для параметру Бернуллі, яка може бути визначена формулою:

$$\left(\hat{p} + \frac{z^2_{\alpha/2}}{2n} \pm z_{\alpha/2}\sqrt{[\hat{p}(1-\hat{p}) + z^2_{\alpha/2}/4n]/n}\right)/(1 + z^2_{\alpha/2}/n).$$

де: p – доля позитивних оцінок; z – квантіль стандартного нормального розподіду (показник, що характеризує розподіл випадкової величини відносно медіани); n – загальна кількість оцінок.

За цією формулою оцінюється нижня межа долі позитивних оцінок при умовах врахування лише позитивних та негативних оцінок (тобто, не беручи до уваги 5-ти бальну систему оцінювання).

Разом з тим, для визначення рейтингу при застосуванні статистичних залежностей може використовуватися й інший математичний апарат, відомий як Байєсовська оцінка (названа іменем автора Томаса Байєса). Ця оцінка передбачає врахування не лише середнього арифметичного значення оцінок, наданих членами комісій, але і їх кількість:

$$\frac{\text{кол-во голосов}}{\text{кол-во голосов} + n} \times \text{средний балл} + \frac{n}{\text{кол-во голосов} + n} \times 7.2453$$

де 7.2453 – деяка усереднена величина, яка прийнята за основу методу.

Складання рейтингу кандидатів – це головне завдання комісій щодо результатів оцінювання у процесі відбору [15, 19].

Таким чином, існуюча автоматизована система дозволяє забезпечувати укомплектованість особовим складом на необхідному рівні для виконання завдань ОКІ СОУ за призначенням.

Висновки. Таким чином, для успішного управління базою знань в сфері захисту критичної інфраструктури, при впровадженні управління знаннями в якості системи підвищення кваліфікації персоналу СОУ, важливо впроваджувати стратегії, що базуються, з одного боку, на вимогах стандартів [13, 14], з іншого – на впровадженні принципів управління базою знань, як процесу, до якого застосовуються правила керування процесом. Це може включати в себе постійне навчання, створення культури безпеки, співпрацю з іншими організаціями і внутрішнє спілкування, а також вдосконалення процесів управління базою знань.

Впровадження і дотримання правил має забезпечувати і приймати участь керівництво ОКІ СОУ, мають застосовуватися всі можливі технології та технічні засоби, сам процес управління базою знань має бути глибоко інтегрований в бізнес процеси організації.

Персонал має бути мотивований, мати потяг до знань через можливість отримання кар'єрних перспектив та матеріальної винагороди. Перелічені умови, поєднані в автоматизовану систему, дозволять підвищити ефективність діяльності організації і забезпечити захист ОКІ СОУ за умови обмеження в ресурсах.

Список літератури:

1. Закон України Про критичну інфраструктуру. Документ 1882-IX. Редакція від 05.12.2022. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

2. Закон України Про основні засади забезпечення кібербезпеки України. Документ 2163-VIII. Редакція від 17.08.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Кабінет міністрів України. Постанова від 19 червня 2019 р. № 518 Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

4. Вєтров В.І. Модель кадрового менеджменту / В.І. Вєтров, О.В. Вранешич// Оборонний вісник. 2020. № 3, С. 16-21.

5. The Army Strategic Planning Guidance 2006-2023. URL: https://www.hsdl.org/?view&did=443218 (дата звернення: 21.10.2023).

6. Королівський декрет від 28 вересня № 1064/2001, Про ухвалення регламенту процесу оцінювання та просування по службі (документ № 2)

7. Офіційний бюлетень Збройних Сил Франції від 13 листопада № 44 2009 року постійна частина Генеральний штаб. URL: https://www.defense.gouv.fr/

8. Про організацію особового складу у Збройних силах Іспанії (документ № 1; глава II розділу VII «Процес оцінювання» і глава I розділу VIII «Порядок підвищення по службі» // Закон від 18 травня № 17/1999. URL: https://www.defensa.gob.es/ministerio/organigrama/subdef/coperfas/

9. Дослідження проблем управління кар'єрою військовослужбовців з врахуванням вимог до кандидатів на посади в Збройних Силах України. Звіт про НДР (шифр «Паспорт") – К.: НМЦ КП МОУ, 2018.

10. Наказ від 23.09.1994 № 263/121 Про затвердження Переліку робіт, де є потреба у професійному доборі. БУДСТАНДАРТ Online – нормативні документи будівельної галузі України. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=52511 (дата звернення: 21.10.2023).

11. Андрєєва Т. Мотивація людей на роботі. *Управління персоналом* 2005 №4. С. 12.

12. Оболонський А. В. Кадрова політика у федеральній державній службі США: історія і сучасність. *Громадські науки і сучасність*. 2001. № 3. С. 41 – 61.

13. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)

14. Workforce Framework for Cybersecurity (NICE Framework) / R. Petersen та ін. National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/nist.sp.800-181r1 (дата звернення: 19.10.2023).

15. Малихін О. В., Ярмольчук Т. М. Актуальні стратегії навчання у професійній підготовці фахівців з інформаційних технологій. Інформаційні технології і засоби навчання. 2020. Т. 76, № 2. С. 43–57. URL: https://doi.org/10.33407/itlt.v76i2.2682 (дата звернення: 19.10.2023).

16. Пан Л. В., Сисенко Н. В., Абрамович О. К. Концепція управління знаннями як новий напрям менеджменту організацій. Наукові записки. Том 30. Економічні науки, 2004. С.97-102

17. 2013 National Infrastructure Protection Plan | CISA. *Cybersecurity and Infrastructure Security Agency CISA*. URL: https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan (дата звернення: 19.10.2023).

18. Прокопенко О. С., Рибидайло А. А., Васюхно С. І. Застосування технології контролінгу для управління кар'єрою військовослужбовців. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ. 2020. № 1 (68). С. 66–73.

Chumachenko S.M., Popel V.A. A SYSTEMATIC APPROACH TO THE AUTOMATION OF PROCESSES FOR ENSURING PERSONNEL COMPETENCE AT CRITICAL INFRASTRUCTURE FACILITIES OF THE DEFENSE FORCES OF UKRAINE

The publication is devoted to the problems of automating the system of selection and assessment of personnel compliance, which should ensure the safety of critical infrastructure facilities of the Defense Forces of Ukraine.

The article examines the main regulatory documents, requirements for personnel, and ways of assessing the appropriateness of their knowledge, skills, and competencies. The requirements of professional standards developed for the sphere of critical infrastructure of the Defense Forces of Ukraine and information protection are taken into account.

This work aims to identify the basic problems associated with the selection of qualified personnel, assessment of their compliance and determination of the quality of work in activity processes. The materials of the article refer specifically to the critical infrastructure objects of the Defense Forces of Ukraine and consider the features related to the processes of ensuring the security of critical infrastructure.

The results obtained as a result of the analysis of personnel problems in the field of ensuring the safety of critical infrastructure facilities should help the heads of institutions, organizations, enterprises, as well as HR units in the formation and staffing of units, training and placement of personnel.

When preparing the publication, the main normative acts regulating the processes of critical infrastructure protection, the experience of developed countries, primarily the USA and the European Union, security standards (DSTU ISO/EN 27001, NIST Special Publication 800-181) and recommended practices were considered.

The conclusions contain recommendations on the automation of the system of selection, training and advanced training of personnel in the field of protection of critical infrastructure objects, as well as its information and cyber security.

The conclusions of the publication contain recommendations for improving the automation of recruitment and placement procedures, planning professional development, and creating a professional training system based on the knowledge management system.

Key words: *automation, management systems, critical infrastructure protection, personnel competence, information security standards, knowledge, skills, competencies, knowledge management.*