DOI: 10.18372/2310-5461.65.19753
УДК 378.005.94 : 004 (045)

О. К. Юдін, д-р. техн. наук., проф.
Державний науково-дослідний інституту технологій кібербезпеки та захисту інформації, Київ
orcid.org/0000-0002-6417-0768
E-mail: yudin.ок8@gmail.com;

М. Ю. Комаров, PhD, канд. техн. наук,
Державний науково-дослідний інституту технологій кібербезпеки та захисту інформації, Київ
orcid.org/ 0000-0002-5739-8959
E-mail: maxkom32@gmail.com;

Л. Г. Черниш, канд. техн .наук, доцент
Державний науково-дослідний інституту технологій кібербезпеки та захисту інформації, Київ
orcid.org/0009-0004-9264-8863
E-mail: lg4lg666@gmail.com;

В. А. Телющенко
Державний науково-дослідний інституту технологій кібербезпеки та захисту інформації, Київ
orcid.org/0000-0001-6026-5105
E-mail: telyushchenko@bigmir.net

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ПРОФЕСІЙНОЇ АТЕСТАЦІЇ КАДРІВ У СФЕРІ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Підготовка та професійна атестація фахівців у сфері безпеки інформації та кібербезпеки, це основа формування кадрової політики та створення національної системи захисту державних інформаційних ресурсів та критичної інфраструктури України в цілому.

Одним із ключових завдань системи підготовки та перепідготовки персоналу у сфері кібербезпеки та захисту інформації, є оцінка відповідності співробітників їхнім посадовим обов'язкам (інструкціям), що передбачає постійне підвищення та фіксоване визначення (оцінка) рівня знань і навичок кадрового складу організацій, підприємств та установ різних форм власності. Професійна атестація фахівців у сфері кібербезпеки є процесом взаємодії між учасниками операційних процесів світового ІТ суспільства, здійснюваним за допомогою відповідних методів та моделей на основі спеціалізованого програмного забезпечення та апаратно-програмних комплексів [1].

Автоматизовані системи професійної атестації фахівців є складовою частиною системи професійної стандартизації, підготовки та перепідготовки кадрів в сфері кібербезпеки. Оперативний контроль знань і навичок співробітників можливий лише за умови всебічного застосування процедур комп'ютерного тестування, що дозволяють оцінювати рівень підготовки та відповідності фахівців (зрілість персоналу) для виконання визначених безпекових задач у кіберпросторі. Підвищення рівня ефективності комп'ютерного тестування, можливо досягнути завдяки впровадженню адаптивних алгоритмів та моделей створення таких систем, на розробку яких останнім часом приділяється значна увага в світі і нашій державі.

Аналіз останніх досліджень та публікацій

Автоматизовані системи атестації кадрів вже сьогодні використовуються у багатьох країнах, і їх впровадження значно підвищує ефективність процесу управління персоналом. Майбутнє цих систем пов'язане з інтеграцією новітніх технологій, таких як штучний інтелект, машинне навчання, що дозволяє створювати більш адаптивні, прозорі та об'єктивні рішення для оцінки та розвитку кадрів.

Для прикладу, компанія MyKnowledgeMap (Велика Британія) - розробила платформу для автоматизованого оцінювання кваліфікації співробітників та студентів. Вона дозволяє сформувати карту знань, відстежити рівень готовності до екзамену та підвищити ефективність навчання. Активно використовується в освітніх установах та

в корпоративному секторі, зокрема для підвищення кваліфікації працівників.

Дослідженням впровадження автоматизованих систем професійної атестації кадрів займаються вчені та експерти в області управління персоналом, інформаційних технологій, автоматизації бізнес-процесів та управлінських наук. Вони активно працюють над вивченням ефективності таких систем, їхнього впливу на розвиток персоналу і на оптимізацію робочих процесів в компаніях.

Серед вагомих досліджень вітчизняних вчених в даній сфері можна видіти праці В. Чобіток, О. Кузьмін, А. Колот, І. Дашко, Ю. Сотнікова, О. Мельник, Л. Саркісян, В.Лугова, В. Пономаренко, І. Журавльова, тощо.

У науковій статті доктора економічних наук, професора кафедри управління персоналом і маркетингом Запорізького національного університет І. Дашко (2022 рік) проаналізовано необхідність впровадження сучасних систем автоматизації при атестації працівників на підприємствах [1].

Також застосування сучасних систем і технології при формуванні системи оцінки персоналу на підприємстві розглядалося у статті кандидата економічних наук, доцента кафедри економіки та організації діяльності суб'єктів господарювання Української інженерно-педагогічна академії В. Чобіток. Вона заначила, що впровадження інформаційних технологій при оцінювати рівня підготовки персоналу надасть можливість підвищити рівень фінансово-економічних, соціально-економічних і кадрових показників [2].

Автори О. Мельник та Л. Саркісян обґрунтували необхідність впровадження інноваційних методів управління персоналом.

Незважаючи на значні дослідження щодо необхідності впровадження автоматизованих систем сертифікації персоналу на сьогодні необхідним є вдосконалення механізму професійної атестації фахівців у сфері кібербезпеки та захисту інформації.

Постановка проблеми

Метою статті є дослідження сучасних методів та моделей створення та впровадження автоматизованої системи професійної атестації (сертифікації) кадрів у сфері кібербезпеки та захисту інформації, а також розглянуто основні вимоги та задачі комп'ютерного оцінювання знань, вмінь та навичок для професійної атестації фахівців.

Також до мети статті відноситься аналіз та розробка методів та моделей забезпечення процедур присвоєння/підтвердження професійної кваліфікації, базових компонент та топології автоматизованої системи і її мережі для комп'ютерного оцінювання (тестування) фахівців у галузі кібербезпеки.

Виклад основного матеріалу

1. Аналіз сучасного програмного забезпечення та базових вимог для розробки автоматизованих систем тестування

Перед тим, як розглядати базові компоненти автоматизованої системи професійної атестації кадрів розглянемо перелік технічних вимог до програмного забезпечення, а також проведемо аналіз існуючих платформ, що використовуються при комп'ютерному тестуванні та оцінюванні рівня знань вмінь та навичок фахівців.

Враховуючи світовий, вітчизняний та власний досвід побудови АС комп'ютерного тестування (далі – АСТ) авторський колектив сформував базові вимоги до зазначених інформаційних систем достатнього рівня функціональної відповідності та забезпечення гарантій безпеки, а саме:

I. Програмна платформа повинна забезпечувати поєднання (сумісність, синхронізацію) спеціалізованого ПЗ з відомими і стандартизованими системами базами даних за стандартом ISO/IEC 2382:2015x, такими як: MySQL, PostgreSQL, Microsoft SQL Server, Oracle, Sybase, Interbase, Firebird та IBM DB2. Зрозуміло , що повинно враховувати фінансову складову проекту: цінова політика ліцензованого програмного продукту та можливість використання freeware платформ з достатнім рівнем якості виконання проекту.

II. Можливість створення зовнішнього інтерфейсу для АС тестування у вигляді Веб-сайтової політики з метою розробки зручного інтерфейсу та ефективного соціально-інформативного сприйняття системи тестування. Треба враховувати при проектування АС тестування. Що в даному випадку розширюється перелік складових щодо сумісності складових ПЗ, а саме:

– спеціалізоване ПЗ для створення системи тестування з урахуванням формування бази тестових питань;

– використання ПЗ бази даних, котра повинна бути сумісною (синхронізованою) з ПЗ зовнішнього інтерфейсу Веб-сайтової політики.

III. Можливість створення та подальшої атестації комплексної системи захисту інформації для автоматизованої системи атестації з класом АС другого або третього класу згідно чинного законодавства та нормативно-правовою базою держави.

IV. Згідно чинного законодавства України, обов'язкове оформлення договорених відносин щодо ліцензійного використання програмних продуктів для створення АС тестування та побудови інформаційно-комунікаційної системи та мережі.

Автоматизовані системи тестування є критично важливим інструментом для ефективної оцінки знань та навичок фахівців і студентів. Сучасні

програмні рішення та платформи пропонують розширені можливості для створення гнучких, ефективних та безпечних АСТ. Одним з ключових аспектів при розробці інформаційної системи, є сумісність АСТ з базами даних типу SQL для надійного зберігання та управління даними, а також забезпечення високого рівня захисту інформаційних ресурсів.

Розглянемо основні тенденції та характеристики сучасного ПЗ для АСТ. Зрозуміло, що порівняльний аналіз характеристик треба робити з урахуванням наявності або сумісності ПЗ з базами даних або безпосередньо з брендами SQL, тощо.

Технічні вимоги та переваги при формуванні сучасної інтегрованої інформаційної системи комп'ютерного тестування:

- використання хмарних технологій: забезпечують масштабованість, доступність та інтеграцію, часто з використанням SQL-баз даних для зберігання інформації;
- модульність та гнучкість АСТ: конструктор тестів з підтримкою різних форматів, з можливістю інтеграції з SQL для зберігання структури та контенту тестів;
- інтеграція з базами даних (включаючи SQL):

– можливість інтеграції з освітніми платформами (LMS), HR-системами та іншими сервісами, використовуючи SQL для обміну даними;

– збереження результатів тестування, інформації про користувачів та тестові завдання у реляційних базах даних (SQL).

- Реалізація концепцій аналітики та звітності (на базі SQL): потужні інструменти аналізу результатів, формування звітів на основі даних, що зберігаються в SQL-базах;
- кібербезпека та захист даних (ключовий аспект):

– захист даних: Використання SQL-серверів з надійними механізмами аутентифікації, авторизації та шифрування даних;

– захист від SQL-ін'єкцій: розробка ПЗ з урахуванням найкращих практик безпечного кодування для запобігання SQL-ін'єкціям;

– контроль доступу: Гранульована система прав доступу до даних та функціоналу АСТ, що реалізується на рівні бази даних та застосунку;

- Аудит дій: реєстрація всіх важливих дій користувачів та адміністраторів в базі даних для відстеження та аналізу інцидентів;
- виконання функції – адаптивність: налаштування складності завдань, часто з використанням даних про попередні результати, що зберігаються в SQL;
- виконання функції – дружній інтерфейс: зручне керування системою, яка на внутрішньому рівні може взаємодіяти з SQL-базами даних;
- підтримка різних типів контенту: збереження та управління різноманітним контентом у базі даних (текст, зображення, посилання тощо).

Наведемо найбільш відомі приклади сучасних програмних платформ та інструментів для створення і супроводження АСТ:

- спеціалізовані LMS з функціоналом тестування: Moodle, Canvas, Blackboard;
- платформи для онлайн-тестування: Kahoot!, Quizizz, Testportal;
- інструменти для розробки тестів: Articulate Storyline, Adobe Captivate.;
- хмарні сервіси для створення опитувань та тестів: Google Forms, SurveyMonkey;
- платформи для автоматизованого оцінювання коду: HackerRank, LeetCode;
- системи прокторингу: Respondus LockDown Browser, ProctorU (для забезпечення чесності тестування).

Однак, враховуючі вимоги, що були визначені вище, авторський колектив надає перевагу ПЗ безпосередньо при його інтеграції з системи управління базами даних MySQL або Microsoft SQL. Враховуючи ліцензійну цінову політику розробника більш приємним варіантом можуть слугувати ПЗ з відкритим кодом, а саме MySQL.

Наведемо приклади сучасних програмних платформ та інструментів (з потенціалом інтеграції з SQL та засобами безпеки):

- спеціалізовані LMS з розширеними можливостями тестування: Moodle, Canvas, Blackboard (часто використовують власні або підтримують зовнішні SQL-бази даних).
- платформи для онлайн-тестування з API для інтеграції: Деякі платформи надають API для інтеграції з власними або зовнішніми SQL-базами даних для розширення функціоналу та безпеки;
- фреймворки для розробки веб-застосунків: Django (Python), Ruby on Rails (Ruby), Laravel (PHP), ALMONDB – надають потужні інструменти для роботи з SQL та забезпечення безпеки;
- спеціалізовані інструменти для створення тестів з можливістю експорту/імпорту даних у SQL: деякі інструменти можуть мати функціонал для експорту/імпорту тестових завдань та результатів у форматі, сумісному з SQL;
- системи управління базами даних (далі – СУБД): MySQL, PostgreSQL, Microsoft SQL Server – використовуються як основа для зберігання даних АСТ з вбудованими механізмами безпеки.

Інтеграція сучасних автоматизованих систем тестування з базами даних типу SQL є ключовим фактором для забезпечення надійного зберігання,

ефективного управління та глибокого аналізу даних. Приділення особливої уваги безпеці на рівні як програмного забезпечення, так і баз даних, є критично важливим для створення захищених АСТ, що забезпечують об'єктивну та чесну оцінку знань і навичок фахівців та студентів.

Для розробки власної автоматизованої системи професійної атестації кадрів у сфері кібербезпеки та захисту інформації, авторами було вибрано базову комбінацію ПЗ з метою реалізації поставлених технічних та організаційно-технічних вимог, а саме: СУБД MySQL, модульне об'єктно-орієнтоване динамічне навчальне середовище Moodle 4.2.3 + та Almondb, яка розроблена на основі теми Moodle Boost. Almondb, вона швидко та легко налаштовується та містить безліч налаштувань.

2. Базові компоненти та задачі автоматизованої системи професійної атестації кадрів

Наступним кроком формування системи професійної сертифікації та атестації кадрів та у відповідності до професійних стандартів і чинного законодавства України, є створення автоматизованої системи та супроводжуючої зазначені процеси комп'ютерного оцінювання знань, вмінь та навичок – інформаційно-комунікаційної системи.

Автоматизована система професійної атестації кадрів повинна здійснювати процедури оцінювання і визнання результатів навчання осіб (зокрема, здобутих шляхом формальної, неформальної або інформальної освіти) з метою присвоєння та/або підтвердження відповідних професійних кваліфікацій (посад) [3].

Треба зауважити, що згідно чинного законодавства, комп'ютерне тестування з метою реалізації процедур присвоєння та/або підтвердження відповідних професійних кваліфікацій (посад), може проводити тільки уповноважений орган, а саме Кваліфікаційний центр за визначеним професійним напрямом [4, 5, 6]:

Кваліфікаційний центр – суб'єкт, уповноважений Національним агентством кваліфікацій здійснювати оцінювання і визнання результатів навчання, здобутих особами шляхом формальної, неформальної або інформальної освіти, присвоєння та/або підтвердження в сфері інформаційної безпеки та кібербезпеки професійних кваліфікацій, визнання в сфері інформаційної безпеки та кібербезпеки професійних кваліфікацій, здобутих в інших країнах, на підставі сертифікату про акредитування такого кваліфікаційного центру, і внесений до Реєстру кваліфікаційних центрів у складі Реєстру кваліфікацій.

Впроваджуючи процеси комп'ютерного тестування щодо виконання процедур присвоєння та/або підтвердження відповідних професійних кваліфікацій (посад), автори пропонують ввести базові визначення з метою формування нормативно-правових понять системи професійної стандартизації та атестації (сертифікації) фахівців у сфері кібербезпеки та захисту інформації.

Базові нормативно-правові та лінгвістичні визначення напряму професійної атестації кадрів:

здобувач – особа, яка подала до Кваліфікаційного центру заяву про присвоєння/підтвердження професійної кваліфікації та представила документи, що підтверджують професійну та освітню кваліфікацію, її віднесення до рівня Національної рамки кваліфікацій відповідно до розділу обраного професійного стандарту (документи, що підтверджують професійну та освітню кваліфікацію, її віднесення до рівня Національної рамки кваліфікацій), обраного для сертифікації стандарту та зареєстрована для проходження сертифікації у встановленому порядку;

процедура оцінювання результатів навчання (далі – процедура оцінювання) – процедура встановлення відповідності обсягу компетентностей здобувача відповідному професійному стандарту, за результатами якої може бути визнано здобуті ним результати навчання і відповідно присвоєно/підтверджено професійну кваліфікацію;

процедура присвоєння/підтвердження професійних кваліфікацій (далі – процедура присвоєння/підтвердження) – визначена Кваліфікаційним центром відповідно до «Порядку присвоєння та підтвердження професійних кваліфікацій кваліфікаційними центрами» [6]. (далі – Регламент), система заходів і вимог щодо строків та порядку оформлення і подання здобувачем документів, проведення Кваліфікаційним центром їх перевірки і процедури оцінювання, оформлення результатів проведених заходів;

процедура визнання – формальне підтвердження Кваліфікаційним центром професійних кваліфікацій, здобутих заявником в інших країнах (регламентується Постановою Кабінету Міністрів України (далі – КМУ) «Про затвердження Порядку визнання в Україні професійних кваліфікацій, здобутих в інших країнах»);

реєстр сертифікатів – база даних про видані суб'єктам оцінювання сертифікати, що зберігається в Єдиній електронній базі Кваліфікаційного центру професійних стандартів в сфері інформаційної безпеки та кібербезпеки; відомості з реєстру сертифікатів Кваліфікаційного центру передаються до реєстру кваліфікацій при секретаріаті Національного агентства кваліфікацій;

сертифікат про присвоєння/підтвердження професійної кваліфікації (далі – сертифікат) – документ, що засвідчує професійну кваліфікацію особи, виданий Кваліфікаційним центром; сертифікат надає можливість претендувати на зайняття відповідної посади (робочого місця) згідно із законодавством.

Процедури оцінювання і визнання результатів навчання здійснюються з урахуванням наявності:

1. «Процедури присвоєння/підтвердження професійної кваліфікації»;

2. «Регламенту процедури комп'ютерного оцінювання» за професійними кваліфікаціями;

3. Наявність контрольно-оцінювальних матеріалів для здійснення процедур оцінювання, а саме набору тестових завдань з метою реалізації «Процедури присвоєння/підтвердження професійної кваліфікації» та виконання «Регламенту процедури комп'ютерного оцінювання»;

4. Наявність матеріально-технічного забезпечення для здійснення процедур комп'ютерного оцінювання, а саме інформаційно-комунікаційної мережі та системи, спеціалізованого програмного та апаратного забезпечення, тощо.

Під час розроблення процедур комп'ютерного тестового контролю надбаних навичок фахівців, однією з основних проблем є рівень ефективності пропонованих процедур оцінки з погляду на точності рівня тестування, порогів оцінювання та валідності повної тестової групи і кожного тесту окремо.

Механізм представлення фахівцю тестових завдань передбачає формування тестового варіанту для атестації з урахуванням випадкового вибору тестів, а також для кожного наступного варіанту атестації, з повної бази тестових завдань. Передбачається, що база даних автоматизованої моделі оцінювання містить усі сформовані запити за варіантами(традиційно: не менш 4 варіантів по 40–60 тестів з повної тестової групи довжиною від 200 до 600 тестів). Результати розрахунків та набраної статистики оцінювання можуть бути представлені, як у табличній, так і в графічній формі.

На даний час, широко використовуються різноманітні платформи для створення систем автоматизованого тестування, які допомагають швидко отримати доступ до навчальних матеріалів, віртуальних полігонів та в тому числі отримати ефективний інструмент оцінювання знань, умінь та навичок шляхом он-лайн або оф-лайн тестування [2, 4, 5].

Авторами наукових досліджень розроблено технологію автоматизації систем тестування в частині формування тестових сесій, а також:

– розроблено власну платформу АС системи комп'ютерного тестування на основі останньої версії ПЗ Moodle 4.2.3 + (модульне об'єктно-орієнтоване динамічне навчальне середовище) для організації і проведення процедур тестування у відповідності до професійних стандартів;

– сформовано та внесені до системи Бази груп тестів з 16 професійних кваліфікацій («Розробник систем захисту інформації», «Адміністратор мереж і систем», «Фахівець з захисту інформації», тощо), а також проведено апробації на основі платформи програмного забезпечення Moodle 4.2.3 + та ПЗ ALMONDB [7, 8, 9].

3. Складові інформаційно-комунікаційної системи та її мережі

3.1. Мета створення та завдання ІКС

Метою створення інформаційно-комунікаційної системи Кваліфікаційного центру є створення технічного (програмного, апаратного, комунікаційного, інформаційного) середовища реалізації процедури встановлення відповідності обсягу компетенцій, знань, вмінь та навичок здобувача відповідному професійному стандарту, за результатами якої може бути визнано здобуті ним результати навчання і відповідно присвоєно/підтверджено професійну кваліфікацію.

Основними завданнями ІКСМ є реалізація процесів комп'ютерного тестування згідно з встановленою процедурою присвоєння/підтвердження у відповідності до професійних стандартів (кваліфікацій) в сфері кібербезпеки та захисту інформації, що передбачає:

– проходження здобувачем процесу комп'ютерного тестування згідно з встановленою Процедурою присвоєння/підтвердження та Регламентом;

– встановлення оцінювачем рівня професійної кваліфікації здобувача на основі результатів комп'ютерного тестування;

– встановлення, в якій мірі набуті та/або вдосконалені здобувачем знання, уміння та навички відповідають діючим професійним стандартам в сфері інформаційної безпеки та кібербезпеки;

– удосконалення процесу планування та організації оцінювання фахівців у відповідності до професійного стандарту в сфері інформаційної безпеки та кібербезпеки;

– реалізація автоматизації збору, зведення та аналізу за визначеними формами та показниками статистичної звітності відповідно до вимог загальнодержавних та відомчих нормативно-правових актів;

– автоматизація операцій обліку здобувачів всіх категорій.

4. Вимоги до АС тестування

4.1. Недоліки сучасного стану автоматизації процесів комп'ютерного тестування

До основних недоліків сучасного стану процесів комп'ютерного тестування згідно з встановленою Процедурою присвоєння/підтвердження професійної кваліфікації Кваліфікаційного центру відноситься:

– відсутність інтегрованого рішення щодо організації та впровадження комп'ютерного тестування у відповідності до професійних стандартів і кваліфікацій у сфері кібербезпеки;

– відсутність автоматизованого обліку слухачів (пошукувачів) професійних кваліфікацій;

– відсутність уніфікованого або спеціалізованого програмного забезпечення для реалізації системи комп'ютерного тестування згідно з встановленою Процедурою присвоєння/підтвердження та обліку результатів процедури присвоєння/підтвердження.

Головним недоліком інформаційних систем автоматизації процесів процедури комп'ютерного оцінювання результатів навчання у відповідності до процедури присвоєння/підтвердження професійної кваліфікації, регламенту процедури оцінювання Кваліфікаційного центру, є відсутність: стандартизованих аналогів з формалізованими характеристиками (правовими, організаційними, технічними) щодо надання послуг, використання програмного забезпечення, збору звітності та статистичних даних, формату та довжини тестових груп комп'ютерного тестування, тощо.

Основні проблеми, які буде розв'язано в результаті створення Системи:

– реалізація процесів комп'ютерного тестування згідно з встановленою процедурою присвоєння/підтвердження Кваліфікаційного центру та у відповідності до професійних стандартів (кваліфікацій) в сфері кібербезпеки;

– стандартизація та формалізація організаційно-технічних характеристик щодо надання послуг у відповідності до процедури присвоєння/підтвердження;

– стандартизація використання спеціалізованого програмного забезпечення з урахуванням різних класів тестів;

– стандартизація використання формату та довжини тестових груп комп'ютерного тестування;

– автоматизація збору, зведення та аналізу за визначеними формами та показниками статистичної звітності відповідно до вимог загальнодержавних та відомчих нормативно-правових актів;

– автоматизація операцій обліку здобувачів всіх категорій у відповідності до професійного напряму.

4.2. Загальні технічні вимоги

Система повинна забезпечувати проведення комп'ютерного оцінювання фахівців у відповідності до професійних стандартів в сфері інформаційних технологій, інформаційної безпеки та кібербезпеки.

Система повинна забезпечувати одночасну та стабільну роботу при здійсненні оцінювання не менше 10 здобувачів та 5 оцінювачів.

В межах реалізації проєкту планується створити Систему, яка повинна включати всі компоненти (складові), необхідні для впровадження програмного забезпечення для проведення комп'ютерного оцінювання Кваліфікаційним центром. Система повинна відповідати вимогам Національних положень (стандартам), наказам Міністерства освіти та науки України.

Система повинна:

– мати модульний принцип побудови;

– використовувати web-технології для доступу користувачів до програмного забезпечення;

– мати клієнтську частину, що працює на різних клієнтських операційних системах, наприклад: Windows та сімейства Linux;

– мати серверну частину, що має можливість функціонування у операційних системах Windows та сімейства Linux/Unix;

– мати єдину ідеологію та програмно-інформаційну платформу побудови окремих його складових (модулів). У якості сховищ даних повинно використовувати бази даних, що побудовані на сучасних промислових технологіях зберігання, обробки, аналізу даних і доступу до них;

– мати клієнт-серверну архітектуру;

– володіти гнучкою і ефективною системою зміни конфігурації, що дозволяє здійснювати налаштування параметрів функціональних модулів без коригування вихідних кодів програм;

– володіти розвинутими засобами адміністрування, що підтримують (забезпечують) централізоване управління;

– мати вбудовані механізми протоколювання процесів та дій, що виконуються користувачами програмного забезпечення, механізми внутрішнього контролю цілісності та відповідності поточної версії програмного забезпечення, централізованого оновлення клієнтського (серверного) програмного забезпечення;

– забезпечувати збереження інформації (даних) від руйнування при різного роду аваріях і збоях.

5. Вимоги до структури та функціонування

5.1. Вимоги до загальної архітектури

Загальна архітектура Системи має передбачати побудову:

– центрального сегменту який забезпечує функціонування основних сервісів Кваліфікаційного центру;

– резервного майданчику для зберігання резервних копій та резервними місцями для проведення комп'ютерного оцінювання;

– майданчику управління Кваліфікаційним центром.

Для забезпечення процедур комп'ютерного тестування (оцінювання) згідно з розробленим порядком присвоєння та/чи підтвердження, методичних рекомендацій комп'ютерного оцінювання фахівців у відповідності до професійних стандартів, сформовано базову топологію інформаційно-комунікаційної системи та її мережі на базі компонентів CISCO. Рис. 1.

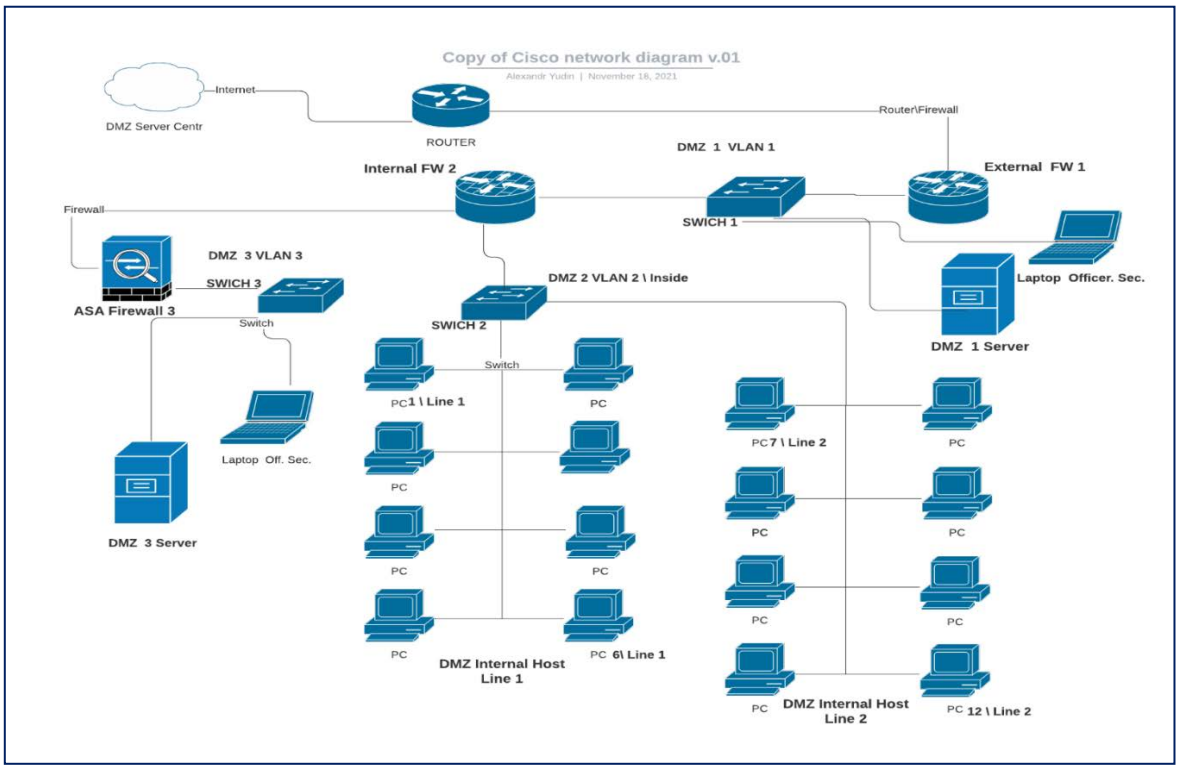

Рис. 1. Приклад топології мережі залу комп'ютерного оцінювання (тестування) фахівців у галузі кібербезпеки

Основні компоненти логічної архітектури Moodle 4.2.3 + та ПЗ ALMONDB включають:

– рівень веб-застосунку, включає в себе веб-інтерфейс, який користується клієнтами (браузерами). Цей шар відповідає за відображення вмісту користувачам та обробку їхніх запитів;

– рівень даних, включає в себе базу даних та обробку даних. Всі дані, необхідні для Moodle, зберігаються та обробляються на цьому рівні.

Moodle є веб-додатком, тому його робота базується на веб-сервері. Веб-сервер отримує запити від клієнтів (браузерів) та відповідає на них, надсилаючи сторінки Moodle. Веб-інтерфейс Moodle взаємодіє з користувачем через його браузер. Користувачі можуть авторизуватися, переглядати курси, виконувати завдання тощо через інтерфейс, який надається веб-сервером.

Для розгортання системи повинно використовуватись серверне обладнання яке забезпечить розгортання на них середовища віртуалізації промислового рівня (VMware ESXi, Hyper-V).

Система повинна будуватись на серверному обладнанні що має характеристики не гірше ніж: процесор – Intel(R) Xeon(R) Gold 5218R CPU @ 2.10GHz 20 Core; оперативна пам'ять – DDR4-3200, 96 Gb; жорсткий диск (SSD) – 2x960 Gb; жорсткий диск (HDD)– 6x2.4 Tb; мережеві адаптери – 6 портів x 1 Гігабіт.

Пропускна спроможність каналу передачі даних у точці підключення серверного обладнання повинна бути не менше ніж 100 Мбіт/с.

Розгортання серверів додатків, баз даних та інших сервісів повинно забезпечуватись у середовищі віртуалізації промислового рівня.

Кількість серверів має забезпечувати безвідмовну роботу Системи у режимі 24/7 та створення копій віртуальних машин на серверному обладнанні розташованому на іншому майданчику з метою швидкого відновлення Системи.

Гіпервізор за допомогою якого створюється середовище віртуалізації повинен забезпечувати:

– віртуалізацію ресурсів: створювати та управляти віртуальними машинами на фізичному сервері відповідно до вимог визначених сервісів;

– ізоляцію та безпеку: віртуальні машини, що працюють у віртуальному середовищі мають бути

ізольовані одна від одної, що забезпечує підвищений рівень безпеки. Це означає, що проблеми, що виникають у одній віртуальній машині, не впливають на інші;

– керування ресурсами: гіпервізор повинен дозволяти ефективно керувати ресурсами сервера, такими як процесор, пам'ять і сховище даних. Це дозволяє адміністраторам встановлювати обмеження та резервування ресурсів для віртуальних машин з метою забезпечення оптимальної продуктивності;

– відмовостійкість: середовище віртуалізації повинно мати вбудовані механізми для забезпечення високої доступності віртуальних машин. Повинна бути забезпечена можливість реплікації віртуальних машин на інші сервери в автоматичному режимі, в разі відмови апаратного забезпечення. Для реплікації допускається використання додаткового програмного забезпечення яке інтегрується з середовищем віртуалізації.

Система має використовувати апаратну або програмну кластеризацію.

Програмні компоненти за допомогою якого створюється середовище віртуалізації повинні дозволяти ефективно управляти та контролювати віртуальні машини та ресурси.

Основні завдання які повинно виконувати програмне забезпечення віртуалізації:

– централізоване управління – повинно мати централізоване місце для керування всіма віртуальними машинами та ресурсами в інфраструктурі. Керування всіма серверами, кластерами, накопичувачами даних та мережами відбувається з одного інтерфейсу;

– керування ресурсами – повинно дозволяти ефективно керувати ресурсами фізичних серверів, такими як CPU, пам'ять та сховища даних, та розподіляє їх серед віртуальних машин відповідно до потреб навантаження;

– управління віртуальними машинами – повинно бути забезпечено керування життєвим циклом віртуальних машин, такими як створення, розгортання, переміщення, резервне копіювання та відновлення;

– моніторинг та звітність – повинно мати засоби моніторингу та звітності, які дозволяють відслідковувати ресурси, моніторити працездатність та аналізувати використання ресурсів;

– доступ до додаткових функцій - розширення функціоналу, управління відмовостійкістю, автоматизація операцій, балансування навантаження, вимоги до ресурсів, резервування та обмеження ресурсів.

У якості операційних систем на ПЕОМ користувачів передбачити використання як ліцензійних версій на базі Windows так і програмного забезпечення з відкритим кодом на базі ядра Linux. Операційні системи ПЕОМ користувачів повинні надавати можливість доступу до програмного забезпечення комп'ютерного тестування через веббраузер (Google Chrome, Opera, Microsoft Edge).

Програмне забезпечення для комп'ютерного тестування повинно бути розгорнуто на базі останньої стабільної версії MOODLE. Операційна система віртуальної машини, на якій буде розгортатися програмне забезпечення, має підтримувати останню версію програмного забезпечення MOODLE.

Операційна система віртуальної машини має підтримувати розгортання одного з наступних веб серверів: Apache, Nginx або Microsoft IIS.

У якості бази даних платформи тестування повинна бути використана одна з баз даних яка забезпечить роботу останньої версії платформи (PostgreSQL, MySQL, MariaDB, Microsoft SQL Server, Oracle Database) MOODLE.

5.2. Вимоги до логічної архітектури

Логічна архітектура Системи визначається відповідно до логіки її функціонування, технологічних процесів та в термінах логічних компонентів, розгорнутих на базі фізичної архітектури Системи. Логічна архітектура Системи включає віртуальні сервери в рамках обчислювального ядра загальної структури

Системи (рівень даних, рівень веб-застосунку, рівень користувача), робоче місце користувачів з веб-доступом.

На серверному рівні Moodle працює як вебдодаток, що використовується для управління навчальним процесом. Ключові аспекти того, як працює Moodle на серверному рівні:

– веб-сервер: Moodle встановлюється на вебсервері, за допомогою Apache, Nginx або Microsoft IIS. Веб-сервер приймає запити від користувачів і відповідає на них, видаючи сторінки Moodle;

– PHP: Moodle написаний мовою PHP і використовується як серверний сценарій для генерації сторінок. Сервер PHP обробляє запити, генеруючи HTML-сторінки на основі вмісту з бази даних Moodle та інших даних;

– база даних: усі дані Moodle зберігаються в базі даних, яка може бути реалізована на системах управління базами даних (СУБД) таких як MySQL, MariaDB, PostgreSQL або MSSQL. Ця база даних містить інформацію про курси, користувачів, завдання, оцінки тощо;

– сеанси та автентифікація: Moodle зазвичай використовує сеанси для управління станом автентифікації користувачів. Користувачі можуть увійти до системи за допомогою різних методів автентифікації, таких як ім'я користувача та пароль, SSO (Single Sign-On), LDAP тощо;

– кешування та оптимізація: Moodle використовує кешування для прискорення завантаження сторінок і покращення продуктивності. Кеш може бути збережений на рівні веб-сервера або може використовуватися спеціальна система кешування, така як Memcached або Redis;

– розширення та додатки: Moodle може бути розширений за допомогою різних додатків, які надають додаткові функції та можливості. Ці додатки можуть бути встановлені через веб-інтерфейс адміністратора Moodle або безпосередньо на рівні сервера.

Основні компоненти логічної архітектури Moodle включають:

– рівень веб-застосунку – включає в себе веб-інтерфейс, який користується клієнтами (браузерами). Цей шар відповідає за відображення вмісту користувачам та обробку їхніх запитів;

– рівень даних - включає в себе базу даних та обробку даних. Всі дані, необхідні для Moodle, зберігаються та обробляються на цьому рівні.

Moodle є веб-додатком, тому його робота базується на веб-сервері. Веб-сервер отримує запити від клієнтів (браузерів) та відповідає на них, надсилаючи сторінки Moodle. Веб-інтерфейс Moodle взаємодіє з користувачем через його браузер. Користувачі можуть авторизуватися, переглядати курси, виконувати завдання тощо через інтерфейс, який надається веб-сервером. Логічна архітектура Системи зображена на рис. 2. .

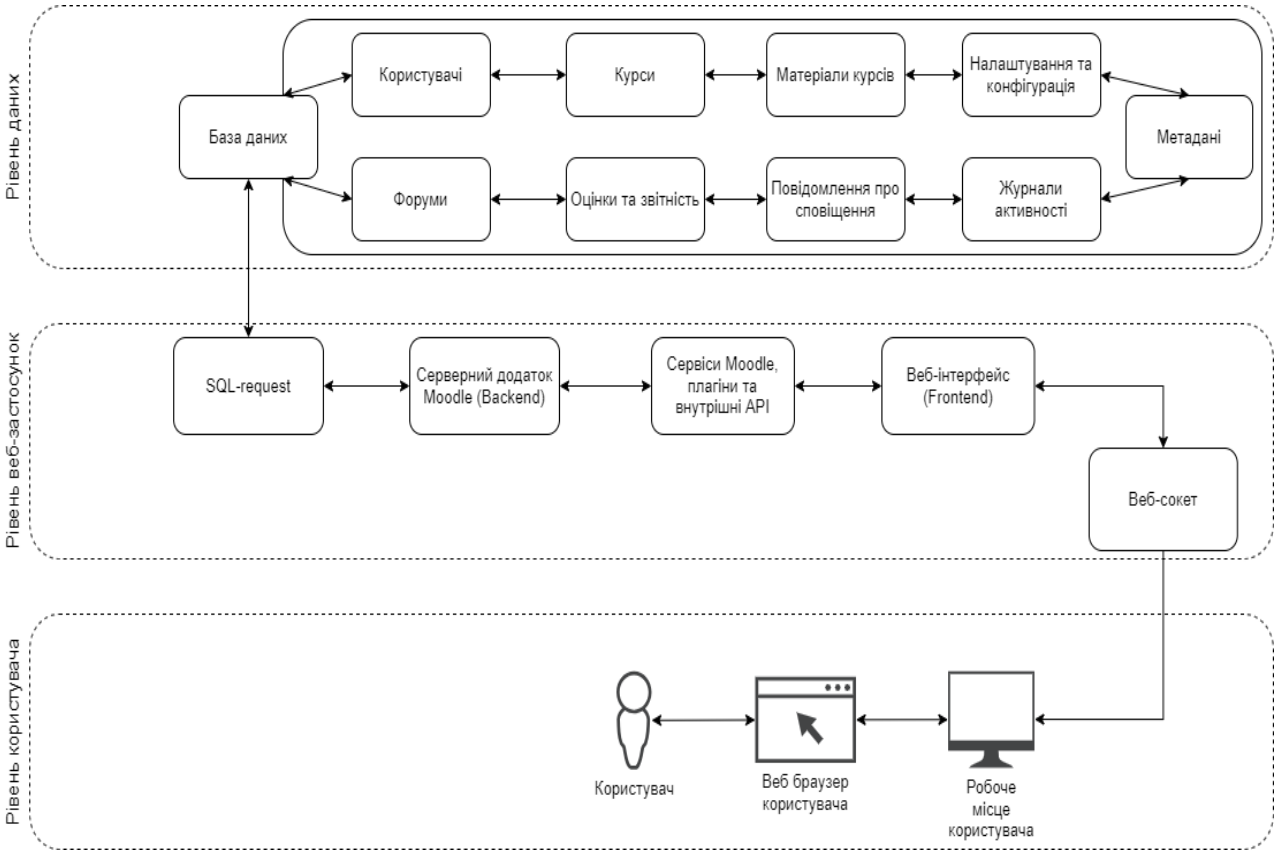

Рис. 2. Логічна архітектура Системи

Зв’язок між компонентами веб-сервера Moodle можна розглядати більш детально на основі взаємодії між веб-сокетом, веб-інтерфейсом Moodle, серверним додатком Moodle, базою даних внутрішніми API та сервісами Moodle.

Етапи взаємодії:

– клієнтський запит - користувачі взаємодіють з Moodle через веб- браузери, надсилаючи HTTP-запити на сервер Moodle. Запити містять URL- адреси та параметри, які визначають, яку сторінку або функціональність запитує користувач;

– веб-сервер отримує HTTP запити від клієнтів та перевіряє ці запити і визначає, до якого додатка або сервісу вони повинні бути направлені;

– веб-інтерфейс Moodle (Frontend) обробляє отримані HTTP-запити, розпізнаючи, яка сторінка або функціонал запитується. Він виконує необхідні операції для підготовки даних, які потрібні для відображення на сторінці;

– веб-інтерфейс взаємодіє з серверним додатком Moodle через внутрішні API та сервіси. Він викликає потрібні методи або сервіси для отримання даних або виконання певних операцій. На-

приклад, для отримання списку курсів використовується відповідний сервіс, який взаємодіє з базою даних та повертає необхідні дані;

– серверний додаток Moodle (Backend) обробляє запити, які отримує від веб-інтерфейсу через внутрішні API та сервіси. Він виконує бізнес-логіку Moodle, таку як обробка запитів, зберігання даних, розрахунок оцінок тощо. Для цього він може звертатися до бази даних для отримання або збереження даних;

– серверний додаток взаємодіє з базою даних для отримання необхідної інформації або збереження нових даних. Зазвичай це включає в себе виконання SQL-запитів до бази даних;

– відповідь для клієнта – після того, як серверний додаток обробив запит та підготував відповідні дані, веб-інтерфейс генерує HTML-сторінку або JSON- відповідь для клієнта. Ця відповідь надсилається назад до веб-сервера, який передає її до браузера користувача

Зв'язок між компонентами веб-сервера Moodle можна розглядати більш детально на основі взаємодії між веб-сокетом, веб-інтерфейсом Moodle, серверним додатком Moodle, базою даних та внутрішніми API та сервісами Moodle. Етапи взаємодії:

– клієнтський запит - користувачі взаємодіють з Moodle через веб- браузери, надсилаючи HTTP-запити на сервер Moodle. Запити містять URL-адреси та параметри, які визначають, яку сторінку або функціональність запитує користувач;

– веб-сервер отримує HTTP запити від клієнтів та перевіряє ці запити і визначає, до якого додатка або сервісу вони повинні бути направлені;

– веб-інтерфейс Moodle (Frontend) обробляє отримані HTTP-запити, розпізнаючи, яка сторінка або функціонал запитується. Він виконує необхідні операції для підготовки даних, які потрібні для відображення на сторінці;

– веб-інтерфейс взаємодіє з серверним додатком Moodle через внутрішні API та сервіси. Він викликає потрібні методи або сервіси для отримання даних або виконання певних операцій. Наприклад, для отримання списку курсів використовується відповідний сервіс, який взаємодіє з базою даних та повертає необхідні дані;

– серверний додаток Moodle (Backend) обробляє запити, які отримує від веб-інтерфейсу через внутрішні API та сервіси. Він виконує бізнес-логіку Moodle, таку як обробка запитів, зберігання даних, розрахунок оцінок тощо. Для цього він може звертатися до бази даних для отримання або збереження даних;

– серверний додаток взаємодіє з базою даних для отримання необхідної інформації або збереження нових даних. Зазвичай це включає в себе виконання SQL-запитів до бази даних;

– відповідь для клієнта - після того, як серверний додаток обробив запит та підготував відповідні дані, веб-інтерфейс генерує HTML-сторінку або JSON – відповідь для клієнта. Ця відповідь надсилається назад до веб-сервера, який передає її до браузера користувача.

Таким чином, зв'язок між компонентами веб-сервера Moodle забезпечує обробку запитів від користувачів, виконання бізнес-логіки та доступ до даних у базі даних, а також відображення результатів для користувачів через веб-інтерфейс.

Для авторизації викладачів та користувачів системи на своїх ПЕОМ необхідно розгорнути OpenLDAP (Open Lightweight Directory Access Protocol). OpenLDAP – це відкрита реалізація протоколу LDAP, який використовується для доступу до каталогів даних. Основне призначення OpenLDAP:

– управління ідентичністю – OpenLDAP використовується для зберігання інформації про користувачів, групи, ролі та інші об'єкти, що використовуються для управління ідентичністю в організації;

– автентифікація та авторизація – OpenLDAP виступає джерелом інформації для автентифікації користувачів під час входу в систему, а також для визначення їхніх прав доступу та ролей;

– централізоване зберігання даних – OpenLDAP надає зручний спосіб зберігати та управляти даними, які можуть бути доступні декільком системам та додаткам.

– розподілена архітектура – OpenLDAP може бути використаний у розподілених системах, де декілька серверів LDAP обслуговують клієнтів у різних місцях мережі;

– синхронізація даних – OpenLDAP може бути використаний для синхронізації даних між різними джерелами та системами, що дозволяє підтримувати єдинообразність інформації у всій організації.

Вимоги до резервування даних

Резервне копіювання віртуальних машин необхідно для можливості відновлення віртуальної інфраструктури у разі збою чи відмови системи. Резервне копіювання та відновлення даних віртуальних машин має відбуватися за допомогою спеціалізованого програмного забезпечення (наприклад Veeam backup & replication). Програмне забезпечення має бути встановлено на окрему віртуальну машину або окрему робочу станцію, яка виступатиме сервером керування резервним копіювання віртуальних машин. На віртуальних машинах встановлюються агенти спеціалізованого програмного забезпечення (якщо вони під-

тримуються) для точного копіювання даних всередині віртуальної машини. Крім цього спеціалізоване програмне забезпечення має копіювати всі конфігураційні файли віртуальної машини безпосередньо у самому гіпервізорі.

6. Політика безпеки АС тестування та базові приклади використання ІКСМ для реалізації пракичних сценаріїв з атестації фахівців у сфері кібербезпеки

Вимоги політики безпеки поширюються на весь персонал Кваліфікаційного центру, включно і на всіх користувачів АС тестування. Усі працівники мають бути ознайомлені із її вимогами. Відповідальність за порушення повинна бути визначена у відповідному розділі затвердженої Політики інформаційної безпеки Кваліфікаційного центру.

Доступ до інформаційних ресурсів закладу через модеми, інші комунікаційні пристрої або відповідне програмне забезпечення підлягає авторизації та автентифікації системою контролю доступу. Зовнішній виклик чи комутація на внутрішній номер (кінцевий пристрій) без проходження через систему контролю доступу повинен бути заборонений.

Системи, що дозволяють проходження зовнішнього виклику на кінцевий пристрій, в тому числі сервер повинні гарантувати додаткову безпеку на рівні операційної системи та додатків. Такі системи повинні також мати можливість контролювати рівень активності, щоб гарантувати, що використання кінцевих пристроїв відбувається належним чином та з виконанням заходів безпеки.

Системи доступу, є базовою складовою забезпечення Політики безпеки. Таким, чином повинні існувати два рівня (підсистеми) доступу: безпосередньо до ІКСМ Кваліфікаційного центру та її ресурсів (віддалений доступ до ІКС, створення особистого кабінету, подача документів з використанням ЕЦП, тощо) та безпосередньо до інформаційних ресурсів АС тестування. Авторизація до інформаційних ресурсів АС тестування проводиться з метою формування та допуску до особистої сесій комп'ютерного тестування у відповідності до визначеної професійної кваліфікації. Приклади стандартизованих вікон для виконання двох етапної процедури авторизації пошукувачів р озроблена на спеціалізованому ПЗ представлено на рис. 3.

Підключення до зовнішніх мереж відбувається через інтернет-провайдера. Якщо користувач має конкретну потребу за процедурою присвоєння\підтвердження зв'язатися із зовнішнім (внутрішнім) компонентом або мережею через прямий канал зв'язку він повинен отримати дозвіл від керівника центру або адміністратора безпеки системи, або іншого відповідального за виконання даних розділів ПБ та пройти процедури подвійної авторизації.

Рівень 1 доступу кінцевих користувачів АС тестування.

Рівень доступу призначений для під'єднання різноманітних пристроїв, такі як робочі станції користувачів, інформаційні мультимедіа термінали, тощо. Рівень доступу кінцевих користувачів забезпечує безпосереднє підключення: робочих станцій користувачів; камер відеоспостереження; інших пристроїв, що використовують ЛОМ.

Активне мережеве обладнання даного рівня проводить розподілення користувачів та пристроїв до відповідних груп в залежності від їх функціонального призначення за допомогою технології віртуальних мереж VLAN. Це дозволяє підвищити безпеку мережі та спростити керування нею.

Повинно бути передбачено використання технології Power over Ethernet (PoE) для спрощення підведення живлення до IP-телефонів, бездротових точок доступу, камер відеоспостереження, та іншого обладнання (використання одного фізичного з'єднання, як для живлення, так і для передачі даних.

Рівень доступу до зовнішніх мереж зв'язку.

Рівень 2 доступу до зовнішніх мереж повинен забезпечувати:

– організацію доступу користувачів до платформи АС тестування з зовнішніх майданчиків користувачів або систем управління Кваліфікаційного центру;

– доступ користувачів системи до інформації в Інтернет, а також для організації безпечного доступу до ресурсів мережі ззовні;

– функціонування системи резервування ресурсів АС тестування.

Обладнання доступу до зовнішніх телекомунікаційних мереж повинно забезпечувати наступні можливості:

– підключення до провайдера Інтернет;

– забезпечення захисту мережевого периметру від внутрішніх та зовнішніх загроз;

– надання безпечного та контрольованого доступу користувачам АС та користувачам гостьових бездротових мереж до мережі Інтернет:

– трансляція адрес приватних мереж у публічні;

– створення політик доступу до мережі Інтернет;

– організація безпечного доступу віддалених користувачів до ресурсів АС.

Для забезпечення захисту мережевого периметру та надання захищеного доступу до ресурсів мережі повинні використовуватись міжмережеві екрани нового покоління.

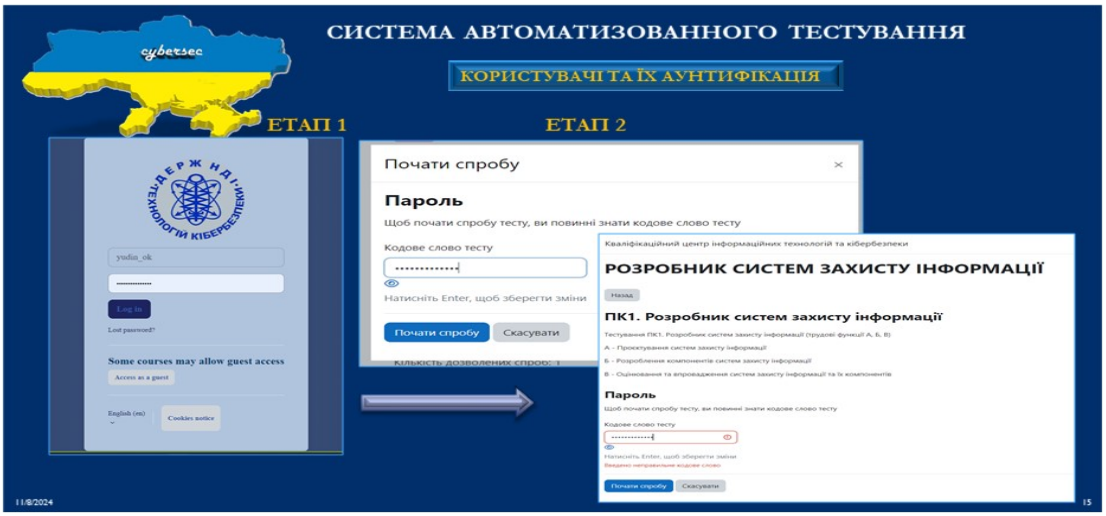

Рис. 3. Приклади стандартизованих вікон для виконання двох етапної процедури авторизації пошукувачів.

Підсистема адміністрування з точки зору виконання вимог ПБ має забезпечувати виконання таких функцій:

– реєстрація, блокування та видалення облікових записів користувачів;

– призначення користувачам первинних паролів на вхід;

– планова та позапланова зміна паролів;

– визначення рольових інтерфейсів адміністраторів з обмеженням доступу цих ролей адміністраторів тільки до певних функцій;

– розмежування доступу користувачів;

– виконання функцій управління списками користувачів та їх функціональними правами (ролями);

– протоколювання та аудит дій користувачів;

– централізоване ведення загальносистемної інформації, обробка облікової інформації;

– розгортання оновлень ліцензованого програмного забезпечення;

– контроль стану та цілісності бази даних користувачів та Тестових груп;

– сповіщення адміністратора про виникнення нештатних ситуацій, тощо.

Права доступу визначаються для ролей користувачів. Користувачу може бути надана одна або одночасно декілька ролей, тим самим для нього буде визначено набір прав доступу до документів, а також доступних до виконання функцій процедур. Відповідно до рівня повноважень, характеру робіт, які виконуються в процесі функціонування ІКС, для адміністраторів та користувачів передбачити відповідні ролі. Перелік ролей та їх повноваження будуть визначені при побудові КСЗІ на АС.

Вимоги щодо захисту інформації.

Контроль та розмежування доступу користувачів до ресурсів АС повинен виконуватись за допомогою налаштування політик доступу. Міжмережевий екран повинен виконувати функції захисту від вторгнень, за допомогою вбудованого функціоналу системи попередження вторгнення.

Міжмережевий екран з системою запобігання вторгнень нового покоління значно підвищує ефективність захисту від загроз і повинен надавати повну контекстну інформацію про користувачів, інфраструктурі, для своєчасного виявлення багатовекторних загроз та автоматизувати процес захисту.

Функціонал міжмережевого екрана повинен дозволяти організовувати різноманітні захищені канали зв’язку для забезпечення захищеного віддаленого доступу користувачів до ресурсів Системи за технологіями VPN.

Система повинна забезпечити захист таких властивостей інформації, як цілісність, доступність та конфіденційність.

З метою забезпечення захисту інформації Система повинна забезпечити:

– авторизацію користувачів

– розмежування прав доступу користувачів до ресурсів (реалізацію рольового керування доступом);

– блокування несанкціонованих дій щодо доступу до даних або до функцій адміністратором безпеки;

– захист цілісності та доступності інформації;

– резервне копіювання та можливість відновлення інформації.

Комплекс засобів захисту має здійснювати програмно-технічну реалізацію політики безпеки у частині:

– забезпечення конфіденційності, цілісності, доступності інформації під час експлуатації за рахунок розмежування доступу та використанням механізмів захисту інформації;

– запобігання спробам відмов користувачів від факту створення інформації;

– створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози та оперативного сповіщення адміністраторів безпеки про факти несанкціонованого доступу до інформації;

– реалізації контролю за роботою користувачів з боку адміністраторів безпеки;

– реєстрації та обробки даних про події, що мають відношення до безпеки інформації;

– забезпечення доступності ресурсів для його авторизованих користувачів.

Комплекс засобів захисту повинен підтримувати функції захисту інформації від несанкціонованого доступу у процесі її обробки компонентами.

Системи та може використовуватися як програмно-технічне ядро комплексної системи захисту інформації в інформаційно-комунікаційних системах класу класу 3 для обробки відкритої інформації.

Базове ліцензійне програмне забезпечення повинно забезпечувати:

Рівень гарантій не нижче Г2 коректності реалізації згідно з НД ТЗІ 2.5-004-99, що підтверджується наданням копії чинного експертного висновку, зареєстрованого в Державній службі спеціального зв'язку та захисту інформації України;

Захист інформації від несанкціонованого доступу у складі ІКС класу "3" відповідно до вимог НД ТЗІ 2.5-005-99, що підтверджується наданням копії витягу з чинного експертного висновку.

Система має надавати комплекс інструментів для створення функціональності та її розвитку без залучення розробника. Тобто розвиток, модернізація та нарощування функціональності може проводитися обслуговуючим персоналом Системи з використанням програмних інструментальних засобів, які є складовою частиною Системи і які не потребують знання мов програмування, наприклад: візуальний конструктор маршрутів (бізнес-процесів), візуальний конструктор функціональних модулів і форм, інші програмні інструментальні засоби Системи.

Висновок

В дослідженнях авторів проведено аналіз актуальності напрямів створення та впровадження автоматизованої системи професійної атестації (сертифікації) кадрів у сфері кібербезпеки та захисту інформації, а також розглянуто основні вимоги та задачі комп'ютерного оцінювання знань, вмінь та навичок для професійної атестації фахівців.

Наведено існуючі методи та моделі забезпечення процедур присвоєння/підтвердження професійної кваліфікації, представлені базові компоненти та приклад топології автоматизованої системи і її мережі для комп'ютерного оцінювання (тестування) фахівців у галузі кібербезпеки.

ЛІТЕРАТУРА

[1] Дашко І. М., Крилов Д. В., Михайліченко Л. В. Атестація персоналу як основний метод оцінювання його розвитку. *Економічний простір*. 2022. № 179. С. 50–54

[2] Чобіток В. І. Формування системи оцінки персоналу на підприємстві: сучасні системи та технології. *Бізнес інформ*. 2019. № 5. С. 192–196.

[3] Кристопчук Т. Стандарти професійної підготовки фахівців у країнах Європейського Союзу та в Україні: порівняльний аналіз. *Неперерв. проф. освіта: теорія і практика*. 2019. № 2 (59). С. 63–67.

[4] Закон України від 05.09.2017 № 2145-VIII «Про освіту».

[5] Закон України від 01.07.2014 № 1556-VII «Про вищу освіту».

[6] Постанова КМУ від 15.09.2021 № 956 «Про затвердження Порядку присвоєння та підтвердження професійних кваліфікацій кваліфікаційними центрами».

[7] Юдін О. К., Черниш Л. Г., Телющенко В. А. Складові автоматизованої системи професійної атестації кадрів у сфері кібербезпеки та захисту інформації: зб. тез доп. науково-практичної конференції «Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки та оборони» 27 вересня 2024 року. Київ : НА СБУ, 2024.

[8] Юдін О. К., Черниш Л. Г., Телющенко В. А. Методи формування бази тестових груп для професійної атестації кадрів у сфері кібербезпеки та захисту інформації.: зб. тез доп. науково-практичної конференції «Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки та оборони» 27 вересня 2024 року. Київ : НА СБУ, 2024.

[9] Юдін О. К., Юдін О. Ю., Черниш Л. Г., Телющенко В. А. Методи імплементації європейської рамки навичок з кібербезпеки при формуванні контенту професійного стандарту «керівник структурного підрозділу з питань безпеки інфор-мації та кіберзахисту. *Наукоємні технології*. 2024. № 2(62). С. 164–173

[10] Мудрук С. Вимоги до апробації екзаменаційних завдань та аналітичний супровід апробації. Методичний посібник. Проект USAID «Справедливе правосуддя».

[11] Mimirinis M. Qualitative differences in academics' conceptions of e-assessment. *Assessment & Evaluation in Higher Education*. 2019. Vol. 44. No. 2. P. 233–248.

[12] Li X. An examination of a gamified E-quiz system in fostering students' reading habit, interest and

ability. *Proceedings of the Association for Information Science and Technology*. 2018. Vol. 55. No. 1. P. 290–299.

[13] Лузан П. Г., Лапа О. В., Пащенко Т. М., Мося І. А., Ваніна Н. М., Ямковий О. О.; за ред. П. Г. Лузана. Методичні рекомендації щодо розроблення валідних тестів у закладах фахової передвищої освіти. Київ: ІПО НАПН України. 2022. 173 с.

[14] Мельник О. Ю., Саркісян Л. Г. Удосконалення системи управління персоналом підприємства. *Вісник Хмельницького національного університету*. 2017. № 6(2). С. 118–122. URL: http://journals.khnu.km.ua/vestnik/pdf/ekon/2009_6_2/pdf/046-051.pdf

[15] НД ТЗІ 2.5-004- 99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

[16] НД ТЗІ 2.5-005- 99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

Юдін О. К., Комаров М. Ю., Черниш Л. Г., Телющенко В. А.

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ПРОФЕСІЙНОЇ АТЕСТАЦІЇ КАДРІВ У СФЕРІ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

У статті досліджено сучасні підходи до розробки та впровадження автоматизованої системи професійної атестації кадрів у сфері кібербезпеки та захисту інформації. Розглянуто методи й моделі оцінювання знань, умінь і навичок фахівців, з метою підвищення ефективності комп'ютерного тестування, як ключового інструменту оцінювання знань, умінь і навичок фахівців.

Авторами розроблено технологію автоматизації систем тестування в частині формування тестових сесій, а також розроблено власну платформу АС системи комп'ютерного тестування на основі останньої версії ПЗ Moodle 4.2.3 +(модульне об'єктно-орієнтоване динамічне навчальне середовище) для організації і проведення процедур тестування у відповідності до професійних стандартів та наведено приклади практичного застосування запропонованих рішень, зокрема створення баз тестових завдань для 16 професійних кваліфікацій та апробацію системи на основі цієї платформи. Значну увагу в статті приділено питанням безпеки даних і забезпеченню захисту інформації в автоматизованих системах, включаючи розмежування доступу, автентифікацію користувачів, резервування даних та дотримання державних стандартів інформаційної безпеки.

Також в роботі описано основні недоліки поточного стану автоматизації атестаційних процесів, серед яких відсутність стандартизованого програмного забезпечення, низький рівень інтеграції систем тестування з професійними стандартами та недостатній контроль за результатами оцінювання.

Результатом роботи є формулювання рекомендацій щодо вдосконалення професійної підготовки кадрів у сфері кібербезпеки в Україні за рахунок впровадження автоматизованої системи атестації персоналу.

Ключові слова: кібербезпека, автоматизована система атестації, комп'ютерне тестування, інформаційна безпека, сертифікація кадрів, професійна кваліфікація, Moodle.

Yudin O., Komarov M., Chernysh L., Telyushchenko V.

DEVELOPMENT OF THE AUTOMATED SYSTEM OF PROFESSIONAL CERTIFICATION OF PERSONNEL IN THE FIELD OF CYBERSECURITY AND INFORMATION PROTECTION

The article investigates modern approaches to the development and implementation of an automated system of professional certification of personnel in the field of cybersecurity and information protection. The methods and models for assessing the knowledge, skills and abilities of specialists aimed at improving the efficiency of computer testing as a key tool for assessing the knowledge, skills and abilities of specialists are considered.

The authors have developed a technology for automating testing systems in terms of forming test sessions, as well as developed their own platform for computer-based testing systems based on the latest version of Moodle 4.2.3 + (modular object-oriented dynamic learning environment) for organizing and conducting testing procedures in accordance with professional standards and provide examples of practical application of the proposed solutions, including the creation of test task bases for 16 professional qualifications and testing the system based on this platform. The article pays considerable attention to data security and information protection in automated systems, including access control, user authentication, data backup, and compliance with state information security standards.

The paper also describes the main shortcomings of the current state of automation of certification processes, including the lack of standardized software, low level of integration of testing systems with professional standards, and insufficient control over the assessment results.

The result of the work is the formulation of recommendations for improving professional training in the field of cybersecurity in Ukraine through the introduction of an automated personnel certification system.

Keywords: cybersecurity, automated certification system, computer testing, information security, personnel certification, professional qualification, Moodle.

Стаття надійшла до редакції 25.12.2024 р.
Прийнято до друку 16.04.2025 р.