УДК 621.3.019.3+004.056

Г.М. ГУЛАК*

МЕТОДОЛОГІЧНІ ЗАСАДИ ПОБУДОВИ ЗАХИЩЕНИХ ГАРАНТОЗДАТНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

*Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. Досліджуються принципи та методи побудови захищених гарантоздатних інформаційних систем (ЗГІС) дистанційного навчання закладів вищої освіти (ЗВО). Проведено аналіз сучасного стану наукових досліджень, практичних розробок та застосування ЗГІС у процесах дистанційного навчання у ЗВО, визначені методологічні засади побудови ЗГІС дистанційного навчання у ЗВО, сформульовані основні завдання ЗГІС для забезпечення повної сумісності дистанційного навчання з очною та заочною формами підготовки студентів, вперше запропонована онтологія сутностей освітнього процесу, що базується на вимогах законодавства про вищу освіту, центральним елементом якої є віртуальне навчальне середовище. На основі застосування побудованої онтології сформовані пріоритетні об'єкти захисту в ЗГІС. У рамках формування моделі загроз для ЗГІС проаналізовані складові її гарантоздатності, надана характеристика їх можливого ураження у випадках реалізації різних загроз, визначені фактори, що впливають на академічну доброчесність учасників освітнього процесу та запропоновані механізми ЗГІС для протидії цим негативним факторам. За методом аналогії побудована модель процедури навчання у рамках окремої навчальної дисципліни, розроблена методика формування змісту тестових контрольних завдань ЗГІС, для чого отримані оцінки раціональної кількості питань у тестовому завданні, ймовірності правильної відповіді на одне тестове питання та випадкового збігу відповідей для здобувачів вищої освіти з різними рівнями компетентності (висока, достатня, середня), а також розрахована межа випадкового збігу результатів тестування, перевищення якої може свідчити про порушення вимог академічної доброчесності. Застосування зазначеної методики у складі ЗГІС може сприяти підвищенню рівня академічної доброчесності.

Ключові слова: гарантоздатність, дистанційне навчання, освітні послуги, компетентність, академічна доброчесність, кібербезпека, криптографічний захист інформації, тестове завдання.

Аннотация. Исследуются принципы и методы построения защищенных гарантоспособных информационных систем (ЗГИС) дистанционного обучения в высших учебных заведениях (ВУЗ). Проведен анализ современного состояния научных исследований, практических разработок и применения ЗГИС в процессах дистанционного обучения в ВУЗах, методологические основы построения ЗГИС дистанционного обучения в ВУЗе, сформулированы основные задания ЗГИС для обеспечения полной совместимости дистанционного обучения с очной и заочной формами подготовки студентов, впервые предложена онтология сущностей образовательного процесса, базирующаяся на требованиях законодательства о высшем образовании, центральным элементом которой является виртуальная учебная среда. На основе применения построенной онтологии определены приоритетные объекты защиты в ЗГИС. В плане построения модели угроз для ЗГИС проанализированы составляющие ее гарантоспособности, дана характеристика их возможного поражения в случае реализации различных угроз, определены факторы, влияющие на академическую добродетель участников образовательного процесса, и предложены механизмы ЗГИС для противодействия таким негативным факторам. По методу аналогии построена модель процедуры обучения в рамках отдельной учебной дисциплины, разработана методика формирования содержания тестовых контрольных заданий ЗГИС, для чего получены оценки рационального количества вопросов в тестовом задании, оценки вероятности правильного ответа на один вопрос теста и случайного

совпадения ответов для соискателей высшего образования с разными уровнями компетентности (высокий, достаточный, средний), а также рассчитана граница случайного совпадения результатов тестирования, превышение которой может свидетельствовать о нарушении норм академической добродетели. Применение предложенной методики в ЗГИС может способствовать повышению уровня академической добродетели.

Ключевые слова: гарантоспособность, дистанционное обучение, образовательные услуги, компетентность, академическая добродетель, кибербезопасность, криптографическая защита информации, тестовое задание.

Abstract. The principles and methods of building secure reliable information systems (SRIS) for distance learning in higher educational institutions are investigated. The analysis of the current state of scientific research, practical development and application of SRIS in the processes of distance learning in universities, the methodological foundations of building SRIS for distance learning at a university, formulated the main tasks of SRIS to ensure full compatibility of distance learning with full-time and part-time forms of student training, the ontology of entities is proposed for the first time educational process, based on the requirements of the legislation on higher education, the central element of which is a virtual learning environment. Based on the application of the constructed ontology, the priority objects of protection in SRIS are determined. In terms of building a threat model for SRIS, the components of its dependability have been analyzed, a characteristic of their possible defeat in the event of the implementation of various threats is given, the factors that flow into the academic virtue of the participants in the educational process have been identified, and SRIS mechanisms have been proposed to counteract such negative factors. By the method of analogy, a model of the learning procedure for a separate academic discipline was built, a methodology for the formation of the content of test control tasks of SRIS was developed, for which an assessment of the rational number of questions in a test task was obtained, an assessment of the probability of a correct answer to one test question and random coincidence of answers for applicants different levels of competence (high, sufficient, medium), and the border of random coincidence of test results was calculated, the excess of which may indicate a violation of the norms of academic virtue. Application of the proposed methodology in SRIS can help to increase the level of academic virtue.

Keywords: dependability, distance learning, educational services, competence, academic virtue, cybersecurity, cryptographic information protection, test task.

DOI: 10.34121/1028-9763-2020-4-148-162

1. Вступ

Питання автоматизації ділових процесів у ЗВО, зокрема, інформаційно-технологічного забезпечення дистанційного одержання вищої освіти вже протягом останніх 30 років є предметом багатьох досліджень і гарячих дискусій науково-педагогічних працівників, а також об'єктом особливої уваги з боку суспільства.

Загалом у цьому напрямі отримані суттєві практичні результати і існує безліч науково-практичних публікацій, зокрема [1–4].

Так, у роботі [1] досліджені принципи і методи підвищення ефективності автоматизації закладів освіти на основі онтологічного підходу, у системному дослідженні [2] проведено ґрунтовний аналіз сучасного стану дистанційного навчання та застосування технологій дистанційного навчання в ЗВО України, визначені технологічні рішення, що сприяють удосконаленню результатів застосування технологій дистанційного навчання у ЗВО. У роботі [3] проведено аналіз систем електронного документообігу з точки зору процесного підходу для оцінки перспектив використання систем автоматизації діловодства в ЗВО, а в роботі [4] наведені дані порівняльного аналізу двадцятки кращих із точки зору користувачів програмних платформ для організації дистанційного (електронного) навчання, у тому числі, для університетського навчання.

У той же час, розвиток подій поточного року, пов'язаних із поширенням карантинних заходів у зв'язку з пандемією COVID-19, свідчить, що протягом перших трьох місяців карантину спостерігалась обмежена готовність навчальних закладів, зокрема, середньої освіти, ефективно проводити повноцінний навчальний процес [5]. Успіхи у цьому напрямі

в ЗВО недостатньо висвітлені у наукових виданнях, але власний досвід викладання автором статті ряду навчальних дисциплін у ЗВО свідчить, що досягнення в переможних посадовців дещо перебільшені.

Слід звернути увагу, що переважна більшість відомих автору проблемних ситуацій у навчальних закладах, пов'язаних із використанням великої кількості різноманітних програмних платформ, орієнтованих на електронне навчання, обумовлені в першу чергу їх неповною відповідністю освітньому процесу, що визначений законами [6, 7], а також недостатньою увагою з боку розробників щодо врахування вимог до захисту інформації та кібербезпеки [8–10].

Зважаючи на те, що системна розробка вихідних технічних вимог до формування захищених гарантоздатних інформаційних систем дистанційного одержання вищої освіти залишилась поза межами багатьох наукових досліджень, у рамках даної роботи з метою створення передумов для побудови сучасного вітчизняного програмно-технічного забезпечення та матеріальної бази ЗВО уявляється доцільним заповнити цю прогалину. Зокрема, необхідно проаналізувати «вузькі місця» існуючих програмних комплексів електронного навчання, сформувати актуальну модель загроз безпеці функціонування захищеної гарантоздатної інформаційної системи дистанційного навчання ЗВО, визначити та обґрунтувати вимоги щодо конкретних методів захисту.

Також необхідно відмітити, що до цього часу у жодній науковій публікації питання функціональної безпеки інформаційних систем дистанційного навчання не розглядалось.

Метою статті є розробка та дослідження методологічних засад побудови ЗГІС дистанційного навчання у ЗВО, включаючи:

- визначення основних завдань ЗГІС за умов забезпечення сумісності різних форм навчання (очна, заочна, дистанційна) здобувачів вищої освіти;
- формування на підставі вимог законодавства про вищу освіту онтології сутностей освітнього процесу як основи побудови ЗГІС;
- аналіз складової гарантоздатності та формування моделі загроз для ЗГІС;
- визначення факторів, що впливають на академічну доброчесність учасників освітнього процесу, та механізмів ЗГІС для протидії цим негативним факторам.

2. Попередні зауваження та визначення

Перш за все, слід звернути увагу, що поняття «автоматизація ЗВО», «створення системи електронного документообігу ЗВО» і «створення захищеної гарантоздатної інформаційної системи дистанційного навчання ЗВО» значною мірою корельовані, але не є тотожними, оскільки мають на меті різні пріоритети в автоматизації бізнес-процесів, різний обсяг завдань і функції створюваної та/або застосованої автоматизованої системи.

У рамках статті під поняттям «гарантоздатна інформаційна система дистанційного навчання закладу вищої освіти» мається на увазі автоматизована система, що забезпечує підтримку освітнього процесу у ЗВО та надання за участю учасників вказаного процесу якісних освітніх послуг відповідно до вимог законодавства протягом встановленого часу. При цьому освітній процес (далі ОП) розглядається як система науково-методичних і педагогічних заходів, спрямованих на розвиток особистості шляхом формування та застосування її компетентностей [6], а учасниками освітнього процесу (далі УОП) у ЗВО є науковці, науково-педагогічні та педагогічні працівники (далі НПП); здобувачі вищої освіти (ЗО) та інші особи, які навчаються у закладах вищої освіти, а також фахівці-практики, які залучаються до освітнього процесу на освітньо-професійних програмах, та інші працівники ЗВО [7].

Згадаємо деякі визначення, що стосуються об'єкта досліджень, зокрема, згідно з [11], гарантоздатністю комп'ютерної системи називається її здатність надавати послуги, яким можна оправдано довіряти. Гарантоздатність є комплексною властивістю, яка вклю-

час безвідмовність, готовність, живучість, функціональну безпеку, цілісність, конфіденційність, достовірність і обслуговуваність.

Також звернемо увагу на визначення законодавства [7], що дають підстави для побудови онтології основних сутностей освітнього процесу:

- освітня (освітньо-професійна) програма (далі ОПП) – єдиний комплекс освітніх компонентів (навчальних дисциплін, індивідуальних завдань, практик, контрольних заходів тощо), спрямованих на досягнення передбачених такою програмою результатів навчання, що дає право на отримання визначеної освітньої або освітньої та професійної кваліфікації;

- результати навчання – знання, уміння, навички, способи мислення, погляди, цінності, інші особисті якості, які можна ідентифікувати, спланувати, оцінити і виміряти та які особа здатна продемонструвати після завершення освітньої програми (програмні результати навчання) або окремих освітніх компонентів; компетентностей (результатів навчання);

- компетентність – динамічна комбінація знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей, що визначає здатність особи успішно соціалізуватися, проводити професійну та/або подальшу навчальну діяльність.

Виходячи з того, що звичайна освітня діяльність здійснюється у спеціально пристосованих та належним чином облаштованих приміщеннях (аудиторіях, класах, лабораторіях, залах, центрах тощо) та на підставі визначення закону, що дистанційна форма здобуття освіти є індивідуалізованим процесом, що відбувається в основному за опосередкованої взаємодії віддалених один від одного учасників освітнього процесу, і, додаємо, у спеціалізованому середовищі, що функціонує на основі сучасних інформаційно-комунікаційних технологій, можливо зробити висновок про необхідність створення відповідного спеціального середовища у кіберпросторі – навчального середовища ЗВО.

З огляду на це, для забезпечення повної сумісності очного та заочного навчання з дистанційним потрібно виконати проєктування віртуальних (електронних) аналогів матеріальних об'єктів звичайного освітнього процесу таким чином, щоб за допомогою інформаційної системи вирішити такі завдання:

- забезпечення надання ЗО освітніх послуг, яким гарантовано можливо довіряти;
- сприяння академічній мобільності, уникненню зайвих складнощів при переході ЗО з однієї форми навчання на іншу;

- підвищення ефективності освітнього процесу шляхом автоматизації рутинних процедур;

- уникнення негативного впливу інформаційної системи дистанційного навчання на психофізичний стан ЗО;

- зменшення ризиків можливих втрат внаслідок кібератак на інформаційну структуру освітнього процесу, а також незаконних навмисних або випадкових дій його учасників. При цьому має бути забезпечено юридичну силу електронних документів відповідно до вимог законодавства [8–10, 12].

Доцільно відмітити, що питання побудови спеціального середовища у кіберпросторі має суттєві відмінності залежно від спеціальності ЗО. Подальше викладання переважно (але не виключно) орієнтується на підготовку спеціалістів у галузі інформаційних (комп'ютерних) технологій і кібербезпеки.

3. Онтологія сутностей інформаційної системи підтримки освітнього процесу та модель загроз

Аналіз та узагальнення вимог законодавчих актів дозволяє побудувати наведену на рис. 1 модель-онтологію сутностей освітнього процесу, яка може бути використана під час проєктування гарантоздатних захищених інформаційних систем дистанційного навчання закла-

дів вищої освіти. У рамках академічної автономії, уставних документів та делегованих іншими органами прав наведена модель може бути уточнена та деталізована для кожного ЗВО окремо.

Центральним елементом наведеної моделі є віртуальне навчальне середовище, на якому базується освітній процес та яке безпосередньо впливає на результати навчання. Складовими освітнього (навчального) процесу, зокрема, є:

- корпоративні сховища знань та ресурсів (бібліотеки навчальних інформаційних ресурсів, прикладних/навчальних, спеціальних програм, моделюючих комплексів тощо);
- плануючі документи та методичне забезпечення навчального процесу (навчальні плани і програми, розклади занять, робочі програми навчальних дисциплін, методичні комплекси для проведення лекцій, семінарів, практичних та лабораторних занять тощо);
- індивідуальні та групові облікові документи навчального процесу (залікові книжки, журнали обліку навчальних груп, залікові та екзаменаційні відомості, звіти державних екзаменаційних комісій тощо);
- документи поточного контролю якості засвоєння навчальних програм (виконані здобувачами вищої освіти контрольні роботи, тести, реферати, курсові та дипломні роботи тощо).

Рисунок 1 – Онтологія сутностей освітнього процесу

Звернемо увагу, що переведення виключно в електронний вигляд плануючих та облікових документів освітнього процесу, а також документів поточного контролю якості засвоєння навчальних програм за умов створення дружніх інтерфейсів та зручних механізмів узагальнення даних у програмному забезпеченні інформаційної системи дистанційного навчання дозволяє скоротити час на виконання рутинних процедур та підвищити ефективність роботи УОП.

Слід підкреслити, що у побудованій моделі довіра до результатів навчання та/або наукових досягнень забезпечується переважно академічною доброчесністю як сукупністю етичних принципів та правил, якими мають керуватися УОП під час навчання, викладання та провадження наукової діяльності [6, 7], чого явно недостатньо для досягнення гарантоздатності інформаційної системи в умовах реалізації вірогідних загроз безпеки антропогенного (далі АЗ), техногенного (далі ТЗ) та природного (ПЗ) характеру.

По-перше, проаналізуємо можливі наслідки реалізації визначених видів загроз. Зауважимо, що до цього часу науковою спільнотою не прийнята парадигма раціональної побудови моделі загроз для гарантоздатності інформаційних систем, тому уявляється доцільним виходити з методологічних засад побудови моделі загроз у випадках забезпечення інформаційної та кібербезпеки.

Виходячи з наведеної на рис. 1 онтології сутностей освітнього процесу та зважаючи на те, що фактично на поточний час для дистанційного отримання освітніх послуг ЗО використовують велике різноманіття пристроїв від відносно простих смартфонів, планшетів і ноутбуків до більш потужних десктопів, можливо зробити висновок, що раціональним вибором для побудови навчального середовища дистанційної системи буде архітектура типу «клієнт-сервер».

Найбільшу цінність у навчальному середовищі мають корпоративні сховища знань та ресурсів, які потребують забезпечення доступності та цілісності, а також облікові документи освітнього процесу (необхідно забезпечити їх цілісність і автентичність), що робить їх пріоритетними об'єктами убезпечення в інформаційній системі.

У табл. 1 наведені складові гарантоздатності інформаційної системи та характеристика їх можливого ураження. Як основні критерії оцінки ураження були обрані критерії впливу на якість освіти та ступінь довіри до освітніх послуг ЗО.

Загрози техногенного характеру для гарантоздатності інформаційних систем освітнього процесу за походженням та можливими наслідками суттєво не відрізняються від інших поширених типів інформаційних систем, окрім властивості функціональної безпеки.

Таблиця 1 – Складові гарантоздатності інформаційної системи та характеристика їх можливого ураження (модель загроз)

№№	Складові гарантоздатності	Вид загрози	Прямі наслідки реалізації загрози	Опосередковані наслідки
1	Безвідмовність	ТЗ, АЗ, ПЗ	Втрата навчального часу, фінансові витрати на відновлення	Вплив на якість навчання, зниження рівня довіри до результатів навчання та/або наукових досягнень
2	Готовність	ТЗ, АЗ	Втрата навчального часу	Вплив на якість навчання, зниження рівня довіри до його результатів
3	Живучість	ТЗ, АЗ	Втрата навчального часу, фінансові витрати на відновлення	Вплив на якість навчання, зниження рівня довіри до результатів навчання та/або наукових досягнень

4	Функціональна безпека	ТЗ, АЗ	Можливі впливи на психофізичний стан ЗО, втрата свідомості, ризику ургентного стану	Суттєве зниження рівня довіри до методології і результатів дистанційного навчання
5	Цілісність	АЗ, ТЗ	Часткове або повне руйнування програмних та/або інформаційних компонент ІС, втрата їх автентичності	Суттєве зниження рівня довіри до результатів навчання та/або наукових досягнень, вплив на якість навчання
6	Конфіденційність	АЗ, ТЗ	Витік персональних даних, іншої інформації з обмеженим доступом	Суттєве зниження рівня довіри до методології і результатів дистанційного навчання
7	Достовірність	АЗ, ТЗ	Руйнування міток автентичності	Суттєве зниження рівня довіри до результатів навчання та/або наукових досягнень
8	Обслуговуваність	ТЗ, АЗ	Понаднормативне зростання витрат на обслуговування ІС	Вплив на якість навчання, зниження рівня довіри до його результатів

Дійсно, відмови технічного обладнання, поєднані із тривалим часом роботи за комп'ютером, можуть підвищити ризики негативного впливу на зір людини, серцево-судинну систему або психоемоційний стан негативних факторів за рахунок підвищеного рівня яскравості зображення або його мерехтіння, незадовільного зовнішнього освітлення, малої контрастності або порушення фокусування, підвищений рівень ультрафіолетового або електромагнітного випромінювання тощо [13]. Шляхи розв'язання вказаної проблеми виходять за рамки даної роботи і потребують специфічних медико-лабораторних досліджень.

Модель порушника безпеки інформаційної системи дистанційного навчання певним чином нагадує модель порушника в банківській сфері, коли співробітник банку та злочинно налаштована особа потенційно можуть утворювати альянс.

Заради об'єктивності слід визнати, що майже кожен із учасників освітнього процесу може бути порушником академічної доброчесності. Потенційно в поведінці посадових осіб ЗВО або ЗО навіть можуть спостерігатись ознаки корупційних дій, обумовлені намаганням отримати неправомірну вигоду за рахунок необ'єктивної оцінки якості засвоєння ЗО тієї чи іншої навчальної дисципліни.

ЗО, який не виконав у повному обсязі навчальну програму, за підтримки співробітників ЗВО може намагатись отримати позитивні оцінки шляхом списування під час виконання контрольних заходів, академічного плагіату у ході виконання курсової або дипломної роботи, підміни або незаконної модифікації облікових документів, а також інших шахрайських дій.

Розв'язання вказаної складної проблеми полягає у площині комплексного підходу до формування доброчесності у суспільстві. У той же час аналіз технологічних складових освітнього процесу та досвід побудови інформаційних систем, у яких забезпечується цілісність, конфіденційність та доступність, а також спостережність процесів дозволяє запро-

понувати ряд вбудованих в ГІС механізмів для протидії негативним факторам, що підривають академічну доброчесність (табл. 2).

Таблиця 2 – Фактори, що впливають на академічну доброчесність УОП, та пропонувані механізми протидії негативним факторам

Фактори підривають академічну доброчесність	Механізми ГІС для протидії негативним факторам
1. Невиконання УОП навчальних планів і програм, пропуск занять	1.1. Захищений автоматизований облік фактичної участі/відвідування/проведення занять
	1.2. Єдиний у рамках захищений автоматизований облік виконання навчальних планів і програм УОП
2. Плагіат у рефератах/курсових/ дипломних роботах, списування (сприяння списуванню або надання преференцій ЗО) під час контрольних заходів	2.1. Антикорупційна/доброчесна методика побудови тестових контрольних завдань, обчислення «індексу доброчесності» як індикатора необхідності забезпечення пильної уваги до УОП
	2.2. Програмно-апаратний розширений облік індивідуальних результатів навчання ЗО у вигляді захищеної криптографічними методами (автентифікація, шифрування, цифровий підпис) електронної залікової книжки та відповідного корпоративного архіву ОП

У наведених у табл. 2 пропозиціях щодо механізмів протидії негативним факторам першого типу (п.1) основний акцент робиться на забезпеченні контролю та захисті цілісності облікових даних, забезпеченні їх авторства та доступності, автентифікації УОП та обмежуванні доступу до інформаційних ресурсів згідно з визначеними уставними документами ЗВО та функціональними обов'язками УОП (пп. 1.1, 1.2). При цьому доступність інформаційних ресурсів, включаючи архівні та поточні облікові дані, в умовах функціонування сучасних ЗВО та їх доступу до глобальних мереж потребує активної протидії криптографічним вірусам [14], зважаючи на те, що сучасні атаки з їх застосуванням можуть мати майже катастрофічні наслідки [15].

Пропозиції (2.1, 2.2) щодо протидії викликам другої групи (п.2 табл. 2) взаємно пов'язані та спрямовані на забезпечення прозорості і відстежуваності технологічних аспектів процедур та процесів оцінювання результатів навчання ЗО.

По-перше (2.1), уявляється доцільним опрацювання питання створення методологічних основ побудови і застосування (включаючи оцінку результатів) для визначення якості засвоєння навчальних дисциплін контрольних тестів таких, що мінімізують ризики порушення канонів академічної доброчесності, зокрема, забезпечують можливість математично коректно свідчити про ймовірне списування та перешкоджати таким спробам. По-друге, характеристики сучасних мікроелектронних засобів дозволяють побудувати захищений від шахрайських електронний аналог залікової книжки ЗО, яка за якістю, достовірністю та обсягом накопичених даних дозволить дійти до нового рівня взаємодії викладача і ЗО, за умов впровадження якого має бути суттєво знижена ймовірність шахрайських дій.

Вивчення аналітичних оглядів сучасних програмних платформ, що пропонуються для використання у системі дистанційного навчання [4, 16, 17], дозволяє зробити висновок, що питання забезпечення інформаційної безпеки та кібербезпеки у таких системах (платформах) або детально не розглядаються, або не згадуються зовсім. Що стосується функціональності багатьох систем, то вона не повністю відповідає визначеному вітчизняним законодавством ОП [6, 7]. Більшість програмних систем, наведених у зазначених оглядах, орієнтовані на професійне навчання персоналу з метою підвищення ефективності

реалізації бізнес-процесів у рамках обраних компаніями напрямів підприємницької діяльності. Це свідчить про актуальність обраного напрямку досліджень.

На поточний час методологія вимірювання досягнутого рівня гарантоздатності інформаційних систем остаточно поки ще не сформована, тому виникає питання щодо інструментів та методики оцінки відповідного рівня для інформаційних систем дистанційного навчання.

Застосування відомих методів і моделей оцінки ефективності навчання персоналу у випадках використання різних інформаційних систем дистанційного навчання у ЗВО не уявляється можливим у зв'язку з вузько специфічною спрямованістю вказаних методів і моделей, зокрема, орієнтацією їх на цілі, завдання та кінцеві результати корпоративного онлайн-навчання [18]. Тому питання вимірювання досягнутого рівня гарантоздатності інформаційних систем дистанційного навчання у ЗВО потребує окремого дослідження.

4. Методологічні засади побудови тестових завдань для захищених ГІС дистанційного навчання

Методологічні основи побудови тестових завдань для контролю якості засвоєння навчальної дисципліни достатньо глибоко та всебічно опрацьовані й вивчаються у рамках відповідних спеціалізацій педагогічного профілю [19–21]. Водночас, слід відмітити, що у наведених джерелах та багатьох аналогічних за напрямом дослідженнях питання конструювання тестів щодо зменшення ризиків для академічної доброчесності не розглядається. Зважаючи на те, що технологічною основою системи дистанційного навчання є комп'ютерні мережі, уявляється доцільним розглянути деякі основні принципи побудови тестових завдань для програмних засобів (ПЗ).

А. Тести слугують для виявлення помилок в ПЗ, які виникли на етапі їх проєкування. Зокрема, згідно із класичною монографією Г. Майерса [22], тестування ПЗ – це процес виконання програми з метою виявлення помилок. Там же з відповідною аргументацією наведені основні принципи тестування:

- i. Опис передбачуваних результатів є частиною тесту.
- ii. Слід уникати тестування ПЗ її автором.
- iii. Необхідно детально вивчати результати тестування.
- iv. Не слід викидати відпрацьовані тести.
- v. Процес тестування у певному сенсі більш творчий, ніж процес створення ПЗ.
- vi. Тест вважається хорошим, якщо він має високу ймовірність виявлення ще не виявленої помилки.
- vii. Тест вважається вдалим, якщо він дозволів виявити ще не виявлену помилку процесу створення ПЗ.
- viii. Тести, засновані на вимогах до ПЗ, мають бути проаналізовані на повноту, тобто визначена множина вимог, які не були піддані тестуванню.

Зазначимо, що в цілому вказані принципи перекликаються з базовими підходами до формування тестових завдань для контролю знань [20, 21].

В. Наступним кроком формування методології побудови тестових завдань для захищених ГІС дистанційного навчання є формування адекватної моделі навчання у рамках окремої навчальної дисципліни та визначення місця тестів у цій моделі.

Каскадна модель – одна з поширених моделей життєвого циклу ПЗ (ліва частина рис. 1) передбачає, що сформовані системні вимоги є основою для формування вимог до ПЗ, останні разом з функціональними вимогами до ПЗ, що висувуються його замовником, є підставою для визначення архітектури ПЗ, яка є сукупністю базових рішень про організацію ПЗ.

Архітектура ПЗ, у свою чергу, є основою для створення програмного коду ПЗ (подання програми на мові комп'ютера), який підлягає тестуванню з метою перевірки його

відповідності заданим вимогам та відсутності помилок проєктування. Тестування може відбуватися за методами «чорного ящика», «білого ящика» або їх комбінації [23]. Зауважимо, що тестування за методом «чорного ящика» відбувається на відміну від «білого ящика» в умовах відсутності інформації про логічну структуру об'єкта тестування і базується тільки на аналізі вхідних і вихідних даних тесту від цього об'єкта. Не важко бачити, що за логікою тестування за методом «чорного ящика» ситуація узгоджується з умовами тестування результатів навчання.

Результати тестування ПЗ в деяких випадках можуть вимагати коригування системних вимог, які обумовлюються апаратною та програмною платформами (операційною системою) комп'ютерної мережі у частині потрібних ресурсів (пам'ять, швидкодія тощо). Аналогічна ситуація і у випадку тестування результатів навчання, оскільки за певних умов може бути потрібним уточнення робочої програми НД (та/або асоційованих з нею документів) і, можливо, ООП.

Виходячи з визначених законом сутностей ОП, а також віртуального середовища ОП – захищеної гарантоздатної інформаційної системи дистанційного навчання (ЗГІС ДН) та з урахуванням відповідних логічних зв'язків як прототипу моделі процесу навчання у рамках окремої навчальної дисципліни (НР ОНД), пропонується обрати каскадну модель ПЗ (рис. 2).

У запропонованій моделі НРОНД інформаційне наповнення віртуального середовища та його використання здійснюються УОП відповідно до ОПП та кожної конкретної робочої програми навчальної дисципліни (НД).

Рисунок 2 – Модель життєвого циклу ПЗ (зліва) та модель навчання у рамках окремої навчальної дисципліни (справа)

С. Контрольні тести є найважливішою складовою інформаційного ресурсу віртуального середовища, а спосіб їх застосування може суттєво вплинути на ефективність оцінки якості навчання, уникаючи корупційних ризиків. Протягом 2010–2020 років у ході викладання в різних ЗВО навчальних дисциплін «Методи побудови та аналізу криптосистем», «Основи криптографічного захисту інформації» та «Криптографічний захист інформації» [24] відпрацьована та пройшла апробацію методика формування змістовної частини тестових контрольних завдань, яка може бути ефективним інструментом перевірки результатів навчання. Розглянемо сутність запропонованої методики.

Крок 1. Розподіл навантаження на модулі та визначення кількості тестів. Виходячи із принципу повноти тестів (Аviii), їх кількість повинна бути достатньою для розкриття основних положень змістового модуля дисципліни, що вивчається. Загальна кількість питань, які включаються у конкретний варіант тесту, не може перевищувати величини $m \leq \frac{T_{нч}}{t_{cp}}$, де $T_{нч}$ – загальний час для проведення тестування, t_{cp} – середній час для опрацювання одного питання тесту.

Крок 2. Оцінка ймовірності правильної відповіді ЗО на запитання тесту. Згадаємо, що за шкалою оцінювання знань ECTS для отримання позитивної оцінки ЗО повинен забезпечити частку правильних відповідей не менш, ніж

$$\frac{60}{100}m = wm, \text{ де } w = 0,6. \quad (1)$$

Твердження 1. Нехай використовується тестове завдання, що містить m запитань, з кожним із них пов'язані дві відповіді, лише одна з них є вірною. Якщо $(1-\alpha)$ ймовірність правильної відповіді не менш, ніж на mw запитань, t_α – квантіль стандартного нормального розподілу ймовірностей $N(0,1)$ [25], у цих умовах ймовірність правильної відповіді ЗО на одне питання p_ϵ є позитивним рішенням такого рівняння:

$$Ap_\epsilon^2 - Bp_\epsilon + C = 0, \quad (2)$$

де коефіцієнти рівняння обчислюються як

$$A = m + t_\alpha^2, \quad B = 2wm + t_\alpha^2, \quad C = mw^2.$$

Доведення. Позначимо ξ – випадкову величину, що дорівнює кількості вірних відповідей на тестові запитання, тоді ймовірність події, яка відповідає випадку $\xi \geq wm$, дорівнює

$$P(\xi \geq wm) = 1 - \alpha. \quad (3)$$

Виходячи з біноміального розподілу величини ξ , отримуємо вираз для ймовірності

$$P(\xi \geq wm) = \sum_{k=q}^m C_m^k p_a^k (1 - p_a)^{m-k}, \quad (4)$$

де $q = [wm]$ – найбільше ціле число, що не перевищує wm .

Функція розподілу величини $\eta = \frac{\xi - E\xi}{\sqrt{D\xi}}$, де $E\xi = mp_a$ і $D\xi = mp_a(1 - p_a)$ є відпо-

відно математичним очікуванням та дисперсією згідно з інтегральною теоремою Муавра-Лапласа [25], для достатньо великого m наближається до функції розподілу стандартного нормального розподілу $N(0,1)$, тому, з урахуванням (2), для ймовірності (3) отримуємо вираз

$$\begin{aligned} 1 - \alpha = P(\xi \geq wm) &= P\left(\frac{\xi - E\xi}{\sqrt{D\xi}} \geq \frac{wm - E\xi}{\sqrt{D\xi}}\right) = \\ &= 1 - P\left(\eta < \frac{wm - E\xi}{\sqrt{D\xi}}\right) \approx 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t_\alpha} e^{-x^2/2} dx. \end{aligned}$$

З останнього виразу отримуємо співвідношення

$$t_\alpha = \frac{wm - E\xi}{\sqrt{D\xi}} = \frac{wm - mp_a}{\sqrt{mp_a(1 - p_a)}}.$$

Після зведення у квадрат обох частин останнього рівняння та перетворення остаточно отримуємо таке рівняння:

$$(m + t_\alpha^2)p_a^2 - (2wm + t_\alpha^2)p_a + mw^2 = 0.$$

Твердження доведено. Таким чином, на основі заданої ймовірності $1-\alpha$ на основі (2) можливо обчислити необхідну ймовірність правильної відповіді на одне питання та зорієнтуватись щодо його складності для ЗО. Оцінка складності запитань (апробація) може бути проведена шляхом опитування ЗО під час семінарських та практичних занять із навчальною групою.

Крок 3. Визначення вимог до змістовної частини (запитань та відповідей) тестів та її формування. З огляду на наведену вище вимогу щодо повноти програмних тестів Aviii тестові завдання для перевірки знань мають містити базові поняття та зв'язки між ними для кожної теми модуля [21].

Зважаючи на обмежену кількість питань у тесті m , відомості щодо об'єктів у процесах, а також їх характеристик, що не включені у перелік питань тестів, доцільно включати як відповіді на питання, які є частиною тестового завдання.

Практичний досвід свідчить, якщо складність питань тесту потрібно визначати з урахуванням розрахованої та апробованої оцінки ймовірності правильної відповіді на одне питання для середнього (репродуктивного) рівня компетентності ЗО, то для більш глибокого оцінювання ЗО на високому (творчому) рівні компетентності [26] поряд з очевидно простими неправильними відповідями доцільно включати нетривіальні неправильні відповіді.

Наприклад, на питання «Які властивості інформації захищаються шляхом криптографічних її перетворень?» пропонуються три відповіді: а) цілісність та авторство (вірна відповідь); б) оперативність та якість (проста невірна відповідь); в) конфіденційність та достовірність (відповідь-пастка). За досвідом можливо відмітити, що навіть дуже добре підготовлені ЗО, внаслідок неуважного читання відповіді, ототожнюють достовірність із підтвердженням невикривленості інформації й намагаються одночасно запропонувати як правильні першу та третю відповіді. Узагальнений практичний досвід створення змісту контрольних тестів для навчальної дисципліни «Криптографічний захист інформації» та споріднених дисциплін наведено у роботі [27].

Сформований варіант завдання назвемо базовим, від буде використаний для створення індивідуального тестового завдання. Кількість базових варіантів визначається змістовним модулем та максимальною (прогнозованою) кількістю ЗО в одній навчальній групі.

Крок 4. Оцінка ймовірності випадкового збігу результатів тестування у різних ЗО в одному варіанті. Отримання такої оцінки надає можливість оцінити «випадковість» збігу результатів тестування та визначити вірогідність списування.

Твердження 2. Нехай $\bar{\theta}_i = (\theta_{i1}, \dots, \theta_{im})$, де $\theta_{ij} \in \{1, 2, \dots, s\}$ вектор відповідей i -го ЗО на питання тестового завдання (m питань по s відповідей). Ймовірність $p_\zeta^{(12)}$ випадкового збігу відповідей $\theta_{1j} = \theta_{2j}$ у двох різних ЗО на однакове j -те питання в одному варіанті тесту дорівнює

$$p_\zeta^{(12)} = p_a^{(1)} p_a^{(2)} + \frac{(1 - p_a^{(1)})(1 - p_a^{(2)})}{s - 1}, \quad (5)$$

де $p_a^{(1)}$, $p_a^{(2)}$ – відповідно ймовірності правильної відповіді на одне питання 1-го та 2-го ЗО. Значення цих ймовірностей розраховується з (2) виходячи з належності ЗО до рівнів компетентності: висока ($w = 0,9$) – категорія «відмінник», достатня ($w = 0,75$) – «хорошист» або середня ($w = 0,6$) – «трієчник».

Доведення твердження здійснюється шляхом прямих обчислень виходячи з рівномірного розподілу помилкових відповідей.

Слід звернути увагу, що максимум імовірності збігу відповіді на одне питання досягається для двох ЗО, що належать до категорії «відмінників».

Твердження 3. Нехай випадкова величина η дорівнює кількості однакових відповідей у результаті тестування навчання обраних двох ЗО. Тоді про не випадковий характер збігу відповідей із рівнем надійності $(1-\alpha)$ свідчить нерівність

$$\eta \geq mp_{\zeta}^{(12)} + t_{1-\alpha} \sqrt{mp_{\zeta}^{(12)}(1-p_{\zeta}^{(12)})}, \quad (6)$$

де $t_{1-\alpha}$ – квантиль стандартного нормального розподілу ймовірностей, що відповідає рівню надійності $(1-\alpha)$, $p_{\zeta}^{(12)}$ – імовірність випадкового збігу відповідей на одне питання обчислюється з (5).

Доведення твердження (6) здійснюється виходячи з біноміального розподілу випадкової величини η із застосуванням інтегральної теореми Муавра-Лапласа.

Крок 5. Формування на основі базових варіантів тестів індивідуальних варіантів.

Застосування незмінного базового варіанта рано чи пізно призведе до «розкриття» вірних відповідей. Зокрема, якщо для двох навчальних груп тестування відбувається згідно з розкладом занять у різний час, існує висока ймовірність того, що номери правильних відповідей будуть передані ЗО, тестування яких відбувається пізніше.

Для суттєвого ускладнення умов «механічного копіювання» результатів для кожного варіанта генеруються набори з $m+1$ перестановок на множині цілих чисел [24], за допомогою яких здійснюється перемішування як послідовності питань базового варіанта (довжина перестановки – m), а також послідовностей відповідей для кожного з питань (m перестановок довжини s по кількості відповідей). Для створення перестановок може бути використаний швидкий алгоритм генерації підстановок заміни [28].

5. Висновки

У статті визначені методологічні засади побудови ЗГІС дистанційного навчання у ЗВО, зокрема:

- визначено основні завдання ЗГІС за умов забезпечення сумісності різних форм навчання (очна, заочна, дистанційна) здобувачів вищої освіти;
- сформовано на підставі вимог законодавства про вищу освіту онтологію сутностей освітнього процесу як основу побудови ЗГІС, центральним елементом якої має бути віртуальне навчальне середовище;
- проведено аналіз складових гарантоздатності та запропоновано модель загроз для ЗГІС, включаючи визначення факторів, що впливають на академічну доброчесність учасників освітнього процесу;
- запропоновано механізми ЗГІС для протидії негативним факторам, модель навчання у рамках окремої навчальної дисципліни та методику побудови тестових завдань ЗГІС, яка включає оцінки раціональної кількості питань у тестовому завданні, ймовірності правильної відповіді на одне тестове питання та випадковий збіг відповідей для здобувачів вищої освіти з різними рівнями компетентності (високий, достатній, середній), а також розраховано межу випадкового збігу результатів тестування, перевищення якої може свідчити про порушення вимог академічної доброчесності. Застосування зазначеної методики у складі ЗГІС може сприяти підвищенню рівня академічної доброчесності.

Подальші дослідження уявляється доцільним спрямувати на розробку методів вимірювання досягнутого рівня гарантоздатності інформаційних систем дистанційного навчання у ЗВО, дослідження ефективних методів захисту ЗГІС, включаючи принципи побудови та захисту електронної залікової книжки як механізму підтримки норм академічної доброчесності.

СПИСОК ДЖЕРЕЛ

1. Шахгельдян К.И. Теоретические принципы и методы повышения эффективности автоматизации образовательных учреждений на основе онтологического подхода: дис. ... д-ра техн. наук: 05.13.06. М.: Институт информатизации образования Российской академии образования, 2009. 474 с.
2. Сисоева С.О., Осадча К.П. Стан, технології та перспективи дистанційного навчання у вищій освіті України. *Інформаційні технології і засоби навчання*. 2019. Т. 70. № 2. С. 271–284.
3. Клишин А.П., Волкова Н.Р., Еремина Н.Л., Мытник А.А., Клыжко Е.Н. Подходы к автоматизации документооборота в вузе. *Вестник НГУ. Информационные технологии*. 2017. Т. 15, № 1. С. 36–46.
4. The Best Learning Management Systems based on Customer Experience. 2020. August 3. URL: <https://elearningindustry.com/directory/software-categories/learning-management-systems/best/customer-experience> (дата звернення: 03.11.2020).
5. Ликарчук И. Об организации дистанционного обучения. 18.03.2020. URL: <https://ru.osvita.ua/blogs/71808/> (дата звернення: 20.10.2020).
6. Про освіту № 2145-VIII: Закон України. *Відомості Верховної Ради*. 2017. № 38–39. Ст. 380.
7. Про вищу освіту № 1556-VII: Закон України. *Відомості Верховної Ради*. 2014. № 37–38. Ст. 2004.
8. Про захист інформації в інформаційно-телекомунікаційних системах № 80/94-ВР: Закон України. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.
9. Про основні засади забезпечення кібербезпеки України № 2163-VIII: Закон України. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
10. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 р. N 373. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-п#Text> (дата звернення: 06.11.2020).
11. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии. *Радиоэлектронні і комп'ютерні системи*. 2006. № 5. С. 7–19.
12. Про електронні довірчі послуги № 2155-VIII: Закон України. *Відомості Верховної Ради*. 2017. № 45. Ст. 400.
13. Какой вред здоровью наносит экран монитора компьютера, ноутбука, планшета или телевизора? 09.09.2019. URL: [https://eco-e.ru/poleznoe/stati/osveshhenie/ekranyi-\(testyi\)/vred-zdorovyu-nanosit-ekran-monitora](https://eco-e.ru/poleznoe/stati/osveshhenie/ekranyi-(testyi)/vred-zdorovyu-nanosit-ekran-monitora) (дата обращения: 19.10.2020).
14. Young A., Yung M. Cryptovirology: extortion-based security threats and countermeasures. *Proceedings 1996 IEEE Symposium on Security and Privacy* (6–8 May 1996, Oakland, CA, USA). USA, Publisher: IEEE DOI: 10.1109/SECPRI.1996.502676 ISBN: 0-8186-7417-2. P. 125–140.
15. Matt Reynolds. Ransomware attack hits 200,000 computers across the globe. 15.05.2017. New Scientist URL: <https://www.newscientist.com/article/2130983-ransomware-attack-hits-200000-computers-across-the-globe/> (дата звернення: 03.11.2020).
16. ТОП 11 бесплатных систем дистанционного обучения для организации электронного обучения персонала 01.03.2018. URL: <https://hr-elearning.ru/top-besplatnykh-sistem-distancionnogo-obucheniya-personala/> (дата обращения: 03.11.2020).
17. Руденко Л. Топ-10 систем для организации дистанционного обучения. 07.10.2020. Центр высшего дистанционного образования России. URL: <https://vuz24.ru/news/o-distantsionnom-obrazovanii/top-10-sistem-dlya-organizacii-distancionnogo-obucheniya> (дата звернення: 03.11.2020).
18. Удовидченко Р.С., Киреев В.С. Сравнительный анализ моделей оценки эффективности обучения персонала. *Современные проблемы науки и образования*. 2014. № 6. URL: <http://www.science-education.ru/ru/article/view?id=16909> (дата обращения: 20.10.2020).
19. Гласс Дж., Стэнли Дж. Статистические методы в педагогике и психологии / пер. с англ. М.: Прогресс, 1976. 495 с.
20. Аванесов В.С. Методологические и теоретические основы тестового педагогического контроля: дис. ... д-ра пед. наук: 13.00.01. Москва, 1994. 339 с.

21. Мамай С.П. Методика составления тестовых заданий: учебн. пособ. Екатеринбург: Изд-во Урал. гос. проф.-пед. ун-та, 2001. 58 с.
22. Майерс Г. Искусство тестирования программ / пер. с англ. М.: Финансы и статистика. 1982. 175 с.
23. Бейзер Б. Тестирование чёрного ящика. Технологии функционального тестирования программного обеспечения и систем. СПб.: Питер, 2004. 320 с.
24. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. В.: ВНТУ, 2011. 198 с.
25. Ширяев А.Н. Вероятность: в 2-х кн. 4-е изд. перераб. и доп. М.: МЦНМО. 2007. Кн. 1. 552 с.
26. Крайнова Е.А. Майорова С.Н. Проектирование учебной дисциплины с позиций качественной подготовки компетентных специалистов. *Современные наукоемкие технологии*. 2005. № 8. С. 54–55. URL: <http://www.top-technologies.ru/ru/article/view?id=23469> (дата звернення: 06.11.2020).
27. Бабенко Т.В., Гулак Г.М., Сушко С.О., Фомичова Л.Я. Криптологія в тестах, задачах та прикладах: навч. посіб. Дніпро: Національний гірничий університет, 2013. 318 с.
28. Гулак Г.М., Бурячок В.Л., Складанний П.М. Швидкий алгоритм генерації підстановок багато-алфавітної заміни. *Захист інформації*. 2017. № 2. С. 173–177.

Стаття надійшла до редакції 12.11.2020