http://www.moderntechno.de/index.php/meit/article/view/meit14-02-076
DOI: 10.30890/2567-5273.2020-14-02-076

# ANALYSIS OF THE LEVEL OF SAFETY IN E-LEARNING SYSTEMS
## АНАЛІЗ РІВНЯ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННОГО НАВЧАННЯ

**Viunenko O.B. / В'юненко О.Б.**
*Ph.D., assistant prof. / к.е.н., доцент*
*ORCID: 0000-0002-8835-0704*
**Tolbatov A.V. / Толбатов А.В.**
*Ph.D., assistant prof. / к.т.н., доцент*
*ORCID: 0000-0002-9785-9975*
*Sumy National Agrarian University, Sumy, 160 Herasym Kondratiev, Sumy, 40021*
*Сумський національний аграрний університет,*
*Суми, вул. Герасима Кондратьєва, 160, 40021*

***Анотація.*** *В роботі розглядаються проблеми конфіденційності, контролю доступу та управління безпекою системи електронного навчання, які в даний час стали актуальними темами для дослідників електронного навчання. Контроль доступу зосереджується на запобіганні несанкціонованого доступу до спільних ресурсів, а виконанню цієї вимоги в системі електронного навчання є необхідною для захисту вмісту, послуг та особистих даних, але в той же час є досить складним процесом, оскільки це постійно впливає на зручність використання додатків електронного навчання.*

***Ключові слова:*** *інформаційна безпека, системи електронного навчання, дистанційна освіта.*

**Вступ**.

Безпека стала однією з ключових наукових областей інформаційно-комунікаційних технологій. Питання безпеки інформації та конфіденційності в середовищі електронного навчання є вирішальними, оскільки більшість користувачів спілкуються через локальні і глобальні комп'ютерні мережі. З іншого боку, розробники виявляють недостатню увагу у цьому плані при розробці систем електронного навчання (СЕН) (e-Learning, LMS). Internet - це основний засіб спілкування в електронному навчанні, який по суті є незахищеним середовищем. Крім того, Internet доступний для всіх, тому він також стає основою для різних несанкціонованих заходів. Завдяки цій взаємопов'язаності дані чи інформація наражаються на велику кількість загроз та вразливостей безпеки систем e-Learning. Це дослідження має на меті дослідити проблеми безпеки, з якими стикається середовище електронного навчання у вищих навчальних закладах (ВНЗ), а також засоби захисту при загрозах інформаційній безпеці для забезпечення ефективного електронного навчального середовища [1] – [16].

**Загрози безпеці в СЕН.**

Користувачі систем e-Learning постійно стикаються з різними ризиками, атаками чи загрозами під час роботи в середовищі електронного навчання, отже, повинен існувати механізм захисту інформації для досягнення конфіденційності, цілісності та доступності. Відповідні заходи можуть включати механізм контролю доступу за допомогою брандмауера, цифрового підпису та біометричної автентифікації. Криптографія та аутентифікація сеансу також є основними методологіями мережевої безпеки та мають безліч застосувань для онлайн-комунікацій та передачі даних. Крім цього,

використання SMS-повідомлень мобільних пристроїв може забезпечити безпечну аутентифікацію та авторизацію для забезпечення цілісності та конфіденційності системи e-Learning [8]. Загалом можна виділити наступні механізми безпеки, які можуть ефективно застосовуватися в СЕН: 1) контроль доступу (брандмауери); 2) біометрична аутентифікація; 3) аутентифікація SMS; 4) криптографія; 5) аутентифікація сесії; 6) пристрої фізичної безпеки [8], [16].

Інформаційна безпека є життєво важливою як для розробки, так і для впровадження СЕН [8], [9], [10], [11], [12], [13], [14], [15] [16], оскільки вона керує доставкою даних між студентами, викладачами та адміністраторами при одночасному доступі до цих даних. СЕН повинні бути захищені не тільки на стороні адміністратора, а також захищати конфіденційність на стороні студентів. Тому існуюча ескалація впровадження електронного навчання в усьому світі вимагає підвищення рівня конфіденційності у навчальному середовищі. Користувачі як зацікавлена сторона мають різні ролі та обов'язки відповідно до свого статусу та навичок. Неоднорідність, яка характеризує цих користувачів, викликає необхідність використання механізму управління доступом на основі ролей (Role Based Access Control) для регулювання дій користувачів у системі. Ці ролі можуть гарантувати, що жоден користувач не може виконувати неприйнятні дії. Оскільки СЕН - це веб-додатки, тому вони успадкували усі вразливості веб-додатків, а також електронне навчання має певні специфічні проблеми, такі як навчально-методична діяльність та співпраця між студентами та викладачами. СЕН постійно стикаються з різними проблемами, відмінними від традиційних веб-додатків.

**Вплив контролю доступу і авторських прав на електронне навчання.**

Більшість розробок СЕН зосереджені на технічному забезпеченні та наданні контенту для електронного навчання, тоді як проблемами безпеки в системі електронного навчання [8], [9], [10], [11], [12], [13], [14], [15], [16] часто нехтували. З точки зору студента, питання безпеки в СЕН мають іншу направленість. Основна увага приділяється формуванню почуття безпеки з метою взаємодії та співпраці між всіма учасниками навчального процесу. Це охоплює необхідність забезпечення конфіденційності та довіри для студентів. Крім того, можливість студента підтримувати "особистий простір" є першорядною, особливо при обміні особистою інформацією, це є обов'язковим для збереження приватного життя студентів. Студент відчув би себе впевненіше при взаємодії та співпраці з іншими, коли існують механізми, щоб створити таку атмосферу конфіденційності та довіри.

У СЕН можуть бути визначені різноманітні загрози, такі як вторгнення в систему несанкціонованих користувачів, несанкціонована зміна даних, підслуховування даних, відмова системних служб та багато інших. Дуже важливо, щоб система електронного навчання була захищена від маніпуляцій. Питання безпеки зазвичай не сприймаються як центральні проблеми в більшості проектів або тому, що системи зазвичай розгортаються в контрольованих середовищах, або тому, що вони застосовують індивідуальний підхід до навчання, не вимагаючи суворих заходів безпеки [16]. Серед проблем безпеки в електронному навчанні існує ще одна важлива проблема - обман в

Internet. Проведені опитування показують, що онлайн-курси мають більший показник обману, ніж в очних курсах, прогрес в технологіях освіти призводить до збільшення шахрайства, більшість студентів вважають, що в Internet - середовищі легше обманювати, ніж при звичайному спілкуванні.

Ще одне питання безпеки електронного навчання, яке насьогодні привертає все більше уваги - це захист авторських прав. Більшість адміністраторів та інструкторів схильні зосереджуватися на одному типі неетичної поведінки, а саме плагіаті. Однак правовласники матеріалів електронного навчання також мають інтерес захищати свій навчальний матеріал від незаконного використання та розповсюдження. Основним недоліком захисту авторських прав у системі e-Learning є те, що захищений авторським правом матеріал повинен бути наданий студентам у цифровій формі. Навіть незважаючи на те, що постачальник навчальних матеріалів може обмежити доступ до них до тих пір, поки користувач не завершить реєстрацію платежів, це не завадить надалі розповсюджувати копії навчального матеріалу незаконним шляхом. Крім захисту конфіденційності користувачів, важливо згадати і захист контенту. Захист контенту e-Learning - це захист цілісності та авторських прав матеріалів курсу. Автентифікація контенту стає однією з найважливіших проблем електронного навчання [8]. Загалом електронне навчання охоплює як веб-дистанційну освіту, так і веб-сайти, які доповнюють навчання в аудиторії. Більшість сайтів-курсів зазвичай пропонують завантаження додаткових текстів, онлайн-форумів, журналів, вікторин тощо. Тому дослідження в сфері безпеки систем електронного навчання повинні бути мультидисциплінарними і поєднувати дуже різні напрямки досліджень.

**Аналіз рівня безпеки в системі електронного навчання Moodle.**

Широке розповсюдження програм e-Learning в роботі з великими та різноманітними групами користувачів створює базу для виникнення різноманітних помилок та шкідливих атак. Можливість швидкої оцінки ризиків для безпеки є особливо важливою для автоматизованої оцінки [16] електронного навчання. При цьому виникають два основних питання: 1) який тип заходів використовується для збереження конфіденційності та цілісності збереженої інформації; 2) чи існують механізми, які можуть запобігти обману під час проведення онлайн-іспитів. У більшості випадків програми електронного навчання розроблені та впроваджені для об'єднання різних служб у єдине ціле з метою виконання складних завдань, які не можуть бути виконані однією службою. Тому усвідомлення загроз та їх контрзаходів є надзвичайно важливим, оскільки електронне навчання являє собою складну систему яка постійно використовує ресурси Internet.

1 вересня 2020 року Центром технологій для навчання та удосконалення (Centre for Learning & Performance Technologies) був опублікований рейтинг Top Tools for Learning сформований на підставі результатів 14-го щорічного опитування, у якому взяли участь 2369 респондентів з 45 країн: 59% респондентів – представники компаній, підприємств і некомерційних організацій, 41% працівники освіти. Опитування проводилось у період карантину, коли дистанційна робота та навчання були нормою [10].

| | PL 20 | WL 20 | Ed 20 |
|---|---|---|---|
| 1 | YouTube | Zoom | YouTube |
| 2 | Google Search | Microsoft Teams | PowerPoint |
| 3 | LinkedIn | Google Search | Zoom |
| 4 | Twitter | YouTube | Google Docs & Drive |
| 5 | Zoom | PowerPoint | Word |
| 6 | WhatsApp | Word | Google Search |
| 7 | Wikipedia | Wikipedia | Google Classroom |
| 8 | Facebook | LinkedIn | Microsoft Teams |
| 9 | PowerPoint | WhatsApp | Google Meet |
| 10 | Word | Google Docs & Drive | WhatsApp |
| 11 | Google Docs & Drive | Excel | Canva |
| 12 | WordPress | Slack | Padlet |
| 13 | Feedly | Trello | Kahoot |
| 14 | LinkedIn Learning | Skype | Excel |
| 15 | Microsoft Teams | Padlet | Google Forms |
| 16 | Gmail | Dropbox | Moodle |
| 17 | Instagram | Mentimeter | Flipgrid |
| 18 | Skype | Kahoot | WordPress |
| 19 | Google Translate | Articulate | Facebook |
| 20 | Google Chrome | OneNote | Wikipedia |

**Рисунок 1 – Top 20 інструментів для e-Learning в 2020 р. (PL/WL/Ed)**

- Інструменти для особистого навчання (Personal Learning/PL) - це цифрові інструменти, які використовуються людьми для власного самовдосконалення, навчання та розвитку;
- Інструменти для навчання на робочому місці (Workplace Learning/WL) - це цифрові інструменти, що використовуються для проектування, надання, включення та/або підтримки навчання на робочому місці;
- Найкращі інструменти для навчання (Education/Ed) - це цифрові інструменти, які використовують викладачі та студенти в коледжах та університетах.

Архітектура програм електронного навчання зазвичай складається з цілого ряду веб-додатків, блогів, тестів та зовнішньо додатків. Масштаби та складність програм електронного навчання значно зросли від рівня розповсюдження навчальних матеріалів до масштабних складних систем, які керують послугами та співпрацею. Програми електронного навчання постають як стандартизований спосіб розробки та впровадження навчальних матеріалів. Вони реалізовані на стандартних платформах, тому успадковують подібні недоліки безпеки, такі як відкритий доступ до публікацій та інші. Тому основним результатом стандартизації процесів електронного навчання є загальне розуміння та виконання семантики, яку вони забезпечують.

Нині існує багато систем управління навчанням (LMS), які широко використовуються в освіті. Система управління навчанням (LMS) - це

програма, яка надає вичерпний набір інструментів для освітян для управління навчальними ресурсами, адміністративними функціями, оцінками та оцінюванням. Основні типи додатків можна поділяють на 3 основні категорії: безкоштовні/відкриті джерела, Internet-сервіси і комерційні. Усі ці програми мають спільні функції, але деякі з них є більш гнучкими та завершеними в певних аспектах, таких як призначення ролей, керування чатами тощо. Використання програм e-Learning відкриває безліч можливостей, але в той же час усі програми є відкритими для значної кількості загроз, оскільки студенти, приватна інформація та ресурси досить вразливимі до різних типів атак [9].

Сьогодні всі знайомі з Moodle ((Modular Object-Oriented Dynamic Learning Environment). У літературі Moodle класифікується як платформа електронного навчання, але як відкритий код, Moodle наражається на багато загроз і вразливостей. Уразливості можна виявити рано, однак їх також можна використати до появи нових патчів. Moodle не завжди вимагає від користувачів повторної аутентифікації через кешування сеансу і не обмежує доступ через URL-адреси. Вона вразлива до комбінованих методик мережевого моніторингу та мережевих веб-атак. Загалом можна розділити ці атаки на дві основні групи - сеансові атаки та design-атаки.

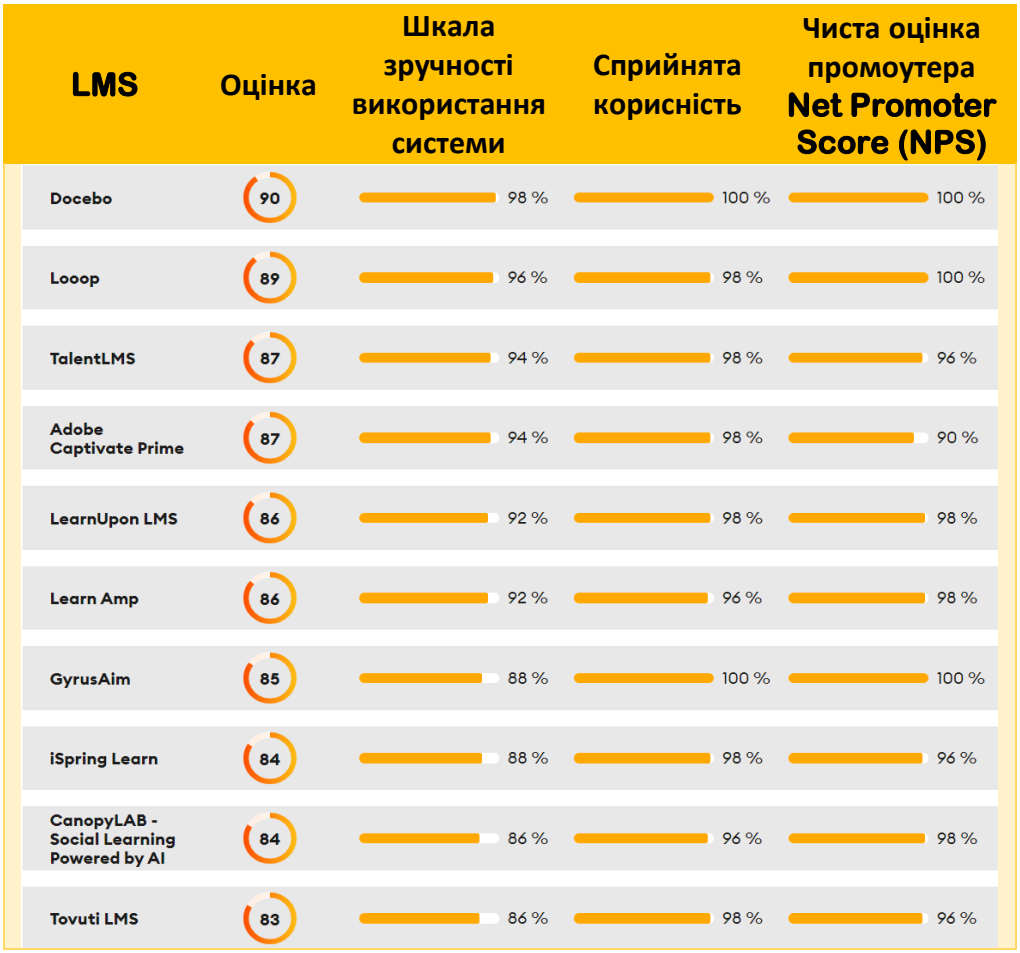


**Рисунок 2 – Top 10 Систем управління навчанням (LMS Software)**

Загальні для Moodle сеансові атаки - це Session Hijacking (перехват сесії) та Session Fixing (фіксація сесії): Session Hijacking - це мало розповсюджена атака,

останніми роками атаки перехвату сеансу були затьмарені шпигунськими програмами, root kits, бот-мережами та атаками типу «відмова в обслуговуванні». Атаки перехвату сеансів визначаються як захват активного сеансу зв'язку TCP/IP без їх дозволу чи відома. Існує три різні типи атак захвату сеансу: активний, пасивний та гібридний. Активна атака - це коли зловмисник викрадає сеанс у мережі. Зловмисник відключає одну з машин, як правило, клієнтський комп'ютер, і займає місце клієнта при обміні даними між робочою станцією та сервером. Активна атака також дозволяє зловмиснику видавати команди в мережі, що дозволяє створювати нові облікові записи користувачів у мережі, які згодом можуть бути використані для отримання доступу до мережі без необхідності виконувати атаку перехоплення сеансу. Пасивні атаки на перехоплення сеансу схожі на активні атаки, але замість того, щоб видаляти користувача з сеансу зв'язку, зловмисник контролює трафік між робочою станцією та сервером. Основна мотивація пасивної атаки полягає в тому, що вона забезпечує зловмиснику можливість контролювати мережевий трафік та потенційно виявляти цінні дані чи паролі. Гібридна атака - це комбінація активних та пасивних атак, які дозволяють зловмиснику прослуховувати мережевий трафік, поки не буде знайдено щось цікаве. Потім зловмисник може модифікувати атаку, видаливши з сеансу комп'ютер робочої станції та підтвердити свою особу [8], [9], [10], [11], [12], [13], [14], [15], [16].

У випадку Moodle ця атака є частиною атак перехоплення, коли зловмисник прослуховує зв’язок між клієнтом та сервером, намагаючись знайти всередині корисні елементи, в цьому випадку HTTP-запит, інформацію якого можна використовувати видаючи себе за користувача і беручи під контроль його сесію. Moodle управляє своїм сеансом через два значення для ідентифікації активного сеансу: MoodleSession та MoodleSessionTest. Ці значення зберігаються у файлі cookie, який надсилається при кожному HTTP-запиті всередині заголовка повідомлення. Для того, щоб видати себе за цільового користувача, зловмисник повинен отримати такі значення. Отримати повні дані HTTP-запиту з включеним файлом cookie дуже просто, оскільки Moodle використовує лише тунелі SSL для служби входу в систему та декількох адміністративних службах. З цієї причини більшість HTTP-запитів виконуються у вигляді простого тексту, який можна перехопити та легко розшифрувати. Отримавши файли cookie, зловмисник може використовувати ці дані у власному HTTP-запиті, взявши під контроль сеанс користувача.

Session Fixing (фіксація сесії) - ця активна атака, яка також націлена на дані сеансу користувача. Замість того щоб прослуховувати зв'язок між цільовим користувачем та сервером зловмисник перехоплює HTTP-запит цільового користувача. Щоразу, коли анонімний користувач отримує доступ до Moodle, надається MoodeSession та MoodleSessionTest. Тому зловмисник може отримати такі значення, як анонімний користувач, а потім перехопити запит цільового користувача, який ще не підтверджено автентифікацією. Після такого перехоплення зловмисник замінює значення MoodleSession та MoodeSessionTest користувача на отримані раніше. Якщо цільовий користувач проходить аутентифікацію, сеанс надається з дозволами користувача, що дає

можливість зловмиснику мати ті ж самі дозволи, оскільки він вже має значення MoodleSession та MoodleSessionTest, які ідентифікують фіксований сеанс.

Найпоширеніші design-атаки в Moodle - це прогнозування пароля (Password Prediction) та прогнозування імені користувача (Username Prediction):

Password Prediction здійснюється шляхом надсилання декількох запитів на сервер Moodle з порожнім полем cookie. Оскільки можлива ситуація, коли кількість помилок входу в систему скидається до нуля, тоді як всередині запиту поле cookie не має значень або взагалі немає файлу cookie, все це може дозволити зловмиснику здійснити атаку методом «грубої сили».

Username Prediction - може бути здійснено двома методами: перехоплення файлів cookie та «грубою силою». При перехопленні файла cookie поле MOODLEID_ може бути декодоване з декодуванням URL та RC4. В свою чергу метод «грубої сили» використовується так як і випадку прогнозування пароля. Однак замість того, щоб надіслати кілька паролів, кілька імен користувачів надсилаються з випадковим паролем. Відповідь Moodle триватиме довше з дійсним іменем користувача, ніж з недійсним, і це може бути використано для розмежування між ними в подібних атаках.

**Висновки.**

Системи електронного навчання отримали нове значення, оскільки технологічний прогрес та бізнес-стратегії постійно змінюються. Електронне навчання змінило свій вектор використання від наукових установ до бізнесу. Хоча люди отримують перевагу від електронного навчання, воно все ще має недоліки, які потрібно враховувати. Більшість нововведень e-Learning були зосереджені на розробці та проведенні курсів, але при цьому майже не враховують приватність та безпеку як необхідні елементи. Поряд із новими технологіями, які прокладають шлях до розвитку та вдосконалення додатків для електронного навчання, кількість загроз та вразливості постійно зростає. Ефективність будь-якого додатка для електронного навчання залежить від того, наскільки добре аспекти безпеки були інтегровані в систему. Конфіденційність, контроль доступу та управління безпекою системи електронного навчання в даний час є однією з актуальних тем для дослідників електронного навчання. Контроль доступу зосереджується на запобіганні несанкціонованого доступу до спільних ресурсів, а виконанню цієї вимоги в системі електронного навчання є необхідною для захисту вмісту, послуг та особистих даних, але в той же час є досить складним процесом, оскільки це постійно впливає на зручність використання додатків електронного навчання.

Література:

1. Вьюненко, А., Толбатов, А., & Агаджанова, С. (2017). Перспективы использования технологии BLOCKCHAIN в учреждениях высшего образования. Modern Engineering and Innovative Technologies, 1(05-01), 84-88. https://doi.org/10.30890/2567-5273.2018-05-01-064

2. Толбатов, В., Толбатов, С., Толбатов, А., Вьюненко, А. 2019. Актуальные вопросы использования технологии BLOCKCHAIN в учреждениях высшего образования. Modern engineering and innovative technologies. 2, 09-02

(окт. 2019), 47-52. DOI: https://doi.org/10.30890/2567-5273.2019-09-02-037.

3. Функції, основні складові та особливості моніторингу дистанційної освіти в ВНЗ / С.В. Агаджанова, О.Б. В'юненко, А.В. Толбатов, К.Х. Агаджанов-Гонсалес, В.А. Толбатов // Науковий журнал Новітні комп'ютерні технології – Кривий Ріг: Видавничий центр ДВНЗ «Криворізький національний університет», 2017. – Том XV. – С. 131–139.

4. Agadzhanova S. et al. Using cloud technologies based on intelligent agent-managers to build personal academic environments in E-learning system //2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). – IEEE, 2017. – С. 92-96.

5. Topical issues of universities' distance e-learning system support [Electronic resource] / A.V. Tolbatov, O.B. Viunenko, G.A. Smolarov, V.A. Tolbatov // Вимірювальна та обчислювальна техніка в технологічних процесах : матеріали XVIII міжнар. наук.-техн. конференції, (м. Одеса, 8-13 червня 2018 р.). - Одеса: Одес. нац. акад. зв'язку ім. О. С. Попова, 2018. – С. 154-157.

6. Tolbatov A. V., Agadzhanova S. V., Tolbatov V. A. Using blockchain technology for E-learning //Вимірювальна та обчислювальна техніка в технологічних процесах. – 2018. – №. 1. – С. 110-113.

7. Akmayeva, G. Impact of access control and copyright in e-learning from user's perspective in the United Kingdom. Brunel University London 2017. P. 17-20.

8. Толбатов А.В. Розробка та підтримка інтелектуальної системи дистанційного навчання у ВНЗ / А.В. Толбатов, В.А. Толбатов, С.В. Толбатов, Д.І. Чечетов // Перспективные инновации в науке, образовании, производстве и транспорте '2013: сб. науч. Тр. Sworld. – Иваново, 2013. – Вып. 4 (13). – С. 18–22.

9. Tolbatov A.V. Modern technologies of distance learning in agrarian higher school / S.V. Ahadzhanova, K.H. Ahadzhanov-Gonsales, A.V. Tolbatov, O.I. Zorenko, V.H. Lohvinenko, N.L. Barchenko, V.A. Tolbatov, S.V. Tolbatov // SW Journal Pedagogy, Psychology and Sociology. – Volume J21508 (9). (November 2015). – P. 109-114. – URL: http://www.sworld.com.ua/e-journal/j21508.pdf

10. Tolbatov A. Mathematical models for the distribution of functions between the operators of the computer-integrated flexible manufacturing systems / Lavrov E., Pasko N., Krivodub A., Tolbatov A. / 2016 Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13 Intern. Conference on TCSET 2016–Lviv-Slavske, 2016. – P. 72–75.

11. Tolbatov A. Data representing and processing in expert information system of professional activity analysis / Zaritskiy O., Pavlenko P., Tolbatov A. / 2016 Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016 – Lviv-Slavske, 2016. – P. 831–833.

12. Tolbatov A. Information technologies in the educational process as the basis of modern distance learning / Viunenko O., Tolbatov A., Vyganyaylo S., Tolbatov V., Agadzhanova S., Tolbatov S. / 2016 Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016 – Lviv-Slavske, 2016. – P. 718–720.

13. Tolbatov A. Development of adaptation technologies to man-operator in distributed E-learning systems / Lavrov E., Pasko N., Barchenko N., Tolbatov A. / 2017 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings – Lviv, 2017. – P. 88–91.

14. Tolbatov A. Cybersecurity of distributed information systems. The minimization of damage caused by errors of operators during group activity / Lavrov E., Tolbatov A., Pasko N., Tolbatov V. / 2017 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings – Lviv, 2017. – P. 83–87.

15. Tolbatov A. Theoretical bases, methods and technologies of development of the professional activity analytical estimation intellectual systems / Zaritskry O., Pavlenko P., Sudic V., Tolbatov A., Tolbatova O., Tolbatov V., Viunenko O. / 2017 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings – Lviv, 2017. – P. 101–104.

16. Tolbatov A. Ergonomic Support for Decision-Making Management of the Chief Information Security Officer / Sergiy Gnatyuk, Nataliia Barchenko, Olena Azarenko, Andrii Tolbatov, Victor Obodiak, Volodymyr Tolbatov / 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019) Lviv Ukraine, November 29, 2019. – P. 459–471.

***Abstract.*** *The paper considers the problems of confidentiality, access control and security management of e-Learning, which have now become relevant topics for e-Learning researchers. Access control focuses on preventing unauthorized access to shared resources, and compliance with this requirement in the e-Learning system is necessary to protect content, services and personal data, but at the same time is quite a complex process because it constantly affects the usability of e-Learning applications.*

***Key words:*** *information security, e-Learning systems, distance education.*