УДК 519.9:004.681
DOI: 10.25140/2411-5363-2020-2(20)-203-209

Юлія Ткач, Михайло Шелест, Леся Черниш, Світлана Литвин, Артур Бригинець

АНАЛІЗ СИСТЕМ ПІДТРИМКИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Актуальність теми дослідження. *Для забезпечення необхідного рівня безпеки інформації на підприємстві необхідно регулярно проводити аудит безпеки інформаційних систем, тому питання аналізу цього процесу є актуальним завданням у сфері кібербезпеки.*

Постановка проблеми. *Нині немає виділеної класифікації, а також аналізу параметрів подібних систем із подальшим їх порівнянням. Тобто відсутня систематизація даних щодо систем підтримки аудиту ІБ, яка повинна дозволити спеціалістам робити більш простий та зважений вибір інструменту для проведення комплексного аудиту, або аудиту інформаційної системи на окремому етапі.*

Аналіз останніх досліджень і публікацій. *Вивченню та систематизації відомостей щодо аудиту та управління інцидентами інформаційної безпеки в Україні присвячено праці багатьох учених, однак питанням різного роду систем підтримки аудиту інформаційної безпеки присвячена недостатня увага українських науковців.*

Виділення недосліджених частин загальної проблеми. *Незважаючи на численні дослідження в напрямку захисту інформації, досі не запропоновано класифікації об'єктів дослідження під час аудиту ІБ підприємства, а також недостатньо проаналізовано сам процес аудиту.*

Постановка завдання. *Актуальним вирішенням вказаних проблем є використання різного роду програмних рішень, які значно полегшують проведення систематизованого аудиту інформаційної безпеки на більшості його етапів, тим самим заощаджуючи ресурси підприємства.*

Виклад основного матеріалу. *Найбільш повного аналізу заслуговують комплексні програми та системи, які охоплюють найбільший спектр можливостей для підтримки аудиту ІБ. Більш спеціалізовані додатки заслуговують об'єму дослідження залежно від реалізованого інструментарію та доцільності в межах аудиту ІБ. Беручи до уваги цілі описаних завдань, можна видилити таку класифікацію об'єктів дослідження з відповідними прикладами: комплексні програми оцінки кіберзагроз у межах мережі, які надають звіт про стан корпоративної мережі, який охоплює ключові загрози ІБ та включає дані про продуктивність і ефективність. Подібні системи дозволяють визначити потенційно вразливі місця та скоригувати політику безпеки організації до настання інцидентів безпеки (Fortinet Cyber Threat Assessment Program); комплексні системи моніторингу дій користувачів, які дозволяють провести внутрішній аудит ІБ, що дозволяє визначити слабкі місця системи захисту інформації та оцінити картину інформаційних потоків на підприємстві (StaffCop Enterprice); програми забезпечення тестування на проникнення на різних його етапах, та мережеві сканери безпеки, зокрема системи виявлення несанкціонованого доступу (Network Intrusion Detection System), які використовуються для фіксації шкідливого трафіку (NMap, XSpider, Snort, Wireshark); засоби розробки та впровадження політик безпеки, які дозволяють проводити розробку політик на основі готових шаблонів, організовувати процеси обговорення, розповсюдження та публікації політик безпеки, а також контролювати інформованість співробітників організації в питаннях ІБ (RUSecure Security Online Support Evaluation); програмні засоби для аналізу ризиків ІБ, які дозволяють здійснювати як кількісний, так і якісний аналіз ризиків, а також містять засоби генерації звітів і формування планів обробки ризиків (RA2, MSAT, vsRisk).*

Висновки відповідно до статті. *Основна мета аудиту ІБ полягає в отриманні найбільш повної та об'єктивної оцінки захищеності інформаційної системи, локалізуванні наявних проблем та розробці ефективної програми побудови системи забезпечення ІБ організації. До основних задач аудиту, вирішення яких можна автоматизувати за допомогою програмних додатків, належать саме завдання реалізації компонентів системи управління ІБ. Також у межах аудиту ІБ або окремим проєктом може бути проведено тестування на проникнення, або пентестинг, що дозволяє перевірити здатність інформаційної системи компанії протистояти спробам проникнення в мережу й неправомірного впливу на інформаційні ресурси.*

Ключові слова: *інформаційна безпека; аудит інформаційної безпеки; СМІБ; управління інцидентами ІБ; пентестинг; аналіз ризиків; захист інформації.*

Бібл: 5.

Актуальність теми дослідження. Розвиток інформаційних систем і технологій відіграє дуже важливу роль у життєвому циклі більшості організацій. Це передбачає наявність таких проблем, як хакери, шкідливі програми, віруси та кіберзлочини. Для забезпечення необхідного рівня безпеки інформації необхідно регулярно проводити аудит безпеки інформаційних систем, але як основні перешкоди на шляху до успішного аудиту часто виникає така проблема, як брак фахівців та відсутність підготовлених структур у сфері інформаційної безпеки. Актуальним вирішенням вказаних проблем є використання різного роду програмних рішень, які значно полегшують проведення систематизованого аудиту інформаційної безпеки на більшості його етапів, тим самим заощаджуючи ресурси підприємства.

Постановка проблеми. Оскільки аудит – це комплекс заходів, в якому задіяний не тільки аудитор, а і представники більшості структурних підрозділів компанії, усі учасники цього процесу повинні бути скоординовані. Але в умовах нестачі кваліфікованих і досвідчених фахівців у галузі аудиту інформаційної безпеки (ІБ) важливо легко обирати та якісно

використовувати системи, які мінімізують їхні зусилля і при цьому максимізують результати проведеної роботи. Нині немає виділеної класифікації, а також аналізу параметрів подібних систем із подальшим їх порівнянням. Тобто відсутня систематизація даних щодо систем підтримки аудиту ІБ, яка повинна дозволити спеціалістам робити більш простий та зважений вибір інструменту для проведення комплексного аудиту, або аудиту інформаційної системи на окремому етапі.

Аналіз останніх досліджень і публікацій. Вивченню та систематизації відомостей щодо аудиту та управління інцидентами інформаційної безпеки в Україні присвячено праці О. Г. Корченко, С. О. Гнатюк, С. В. Казмірчук, В. М. Панченко, С. В. Мельник тощо. Окремо можна виділити роботу О. В. Поповича, в якій приділено увагу основним вимогам проведення аудиту інформаційної безпеки [1]. Однак питанням різного роду систем підтримки аудиту інформаційної безпеки присвячена недостатня увага українських науковців.

Виділення недосліджених частин загальної проблеми. Незважаючи на численні дослідження в напрямку захисту інформації, досі не запропоновано класифікації об'єктів дослідження під час аудиту ІБ підприємства, а також недостатньо проаналізовано сам процес аудиту.

Мета статті. Враховуючи необхідність забезпечення якісного рівня аудиту інформаційної безпеки на підприємстві та важливість вибору необхідного інструменту серед їх великого різноманіття, за мету статті можна виділити проведення аналізу подібних систем, який передбачає розгляд технічних особливостей, опис основних можливостей та їх порівняння, а також формування базової класифікації систем підтримки аудиту.

Виклад основного матеріалу. Найбільш повного аналізу заслуговують комплексні програми та системи, які охоплюють найбільший спектр можливостей для підтримки аудиту ІБ. Більш спеціалізовані додатки заслуговують об'єму дослідження в залежності від реалізованого інструментарію та доцільності в межах аудиту ІБ.

Актуальним прикладом програмно-апаратного комплексу, розробленого у 2016 році, є Fortinet Cyber Threat Assessment Program (CTAP) [2]. Для участі в програмі необхідно заповнити анкету на сайті Fortinet. У співпраці з ключовими партнерами компанія Fortinet на термін до семи днів встановлює в межах корпоративної мережі замовника міжмережевий екран, що відслідковує мережевий трафік, показники продуктивності, активність додатків і користувачів, події безпеки, а також запобігає спроби отримання доступу зловмисниками до найбільш важливих файлів та інформації з баз даних. Процесор FortiASIC на платформі FortiGate реалізує апаратне прискорення механізмів обробки пакетів і перевірки вмісту мережевого трафіку, таких як антивірусний захист, контроль додатків, система запобігання вторгнень (Intrusion Prevention System, IPS), межсетевое екранування [3]. FortiGate налаштовується в мережі замовника, або через порт зеркалювання трафіку комутатора локальної мережі; при цьому не порушується нормальна робота користувачів та додатків.

Зібрані дані обробляються системою централізованого управління подіями, яка розгорнута на серверах компанії. Отримана інформація використовується для отримання кількісної оцінки та аналізу мережевого трафіку, відображення відомостей про вторгнення, функціонуванні шкідливих додатків і проходженні шкідливих файлів, які можуть становити ризик для мережі замовника. Глибокий аналіз можливих загроз спирається на досвід дослідницьких груп компанії. За результатами аналізу замовнику надається звіт про оцінку ризику (CTAP Risk Assessment Report), що містить рекомендації щодо усунення вразливостей мережі, виявлених в процесі перевірки. Звіт містить інформацію про мережеві операції, додатки віддаленого доступу, виявлені шкідливі програми та файли, заблокованих атаках, зафіксованих зверненнях до шкідливим і фішингових веб-сайтів, а також використанні мережевих протоколів і хмарних сервісів (SaaS і IaaS) в графічному вигляді.

Звіт розбитий на кілька розділів. Вступна частина містить інформацію про дату і місце проведення досліджень, їх тривалості, а також опис засобів захисту інформації, що застосовуються міжмережевим екраном. Далі йде перелік рекомендованих дій, що дозволяють підвищити безпеку конкретної мережі, наприклад дії, спрямовані на посилення контролю за недовіреними додатками, споживанням ними ресурсів мережі, та запобігання обходу політик безпеки. Важливим моментом є опис засобів захисту інформації, що дозволяють забезпечити безпеку мережі від кіберзагроз та комплексних атак. Розглянемо детальніше основні розділи, наведені в звіті CTAP:

– розділ «Безпека та запобігання загрозам» містить інформацію про виявлені вразливості додатків, які можна використовувати для проведення кібератаки, а також оцінку роботи брандмауера і ймовірність порушення правил безпеки;

– розділ «Активність користувачів» описує функціонуючі додатки користувачів мережі, соціальні мережі, P2P, обмін миттєвими повідомленнями;

– розділ «Продуктивність і використання мережі» наводить інформацію про те, як необхідно оптимізувати засоби безпеки для оптимальної роботи в мережі на підставі пропускної здатності мережі, пікових навантажень, вимоги до обсягу трафіку, тестах моніторингу та продуктивності;

Загалом, CTAP - це ефективний, швидкий, та безкоштовний спосіб оцінити рівень інформаційної безпеки корпоративної мережі організації за допомогою програмно-апаратного комплексу компанії Fortinet. Такий зовнішній аудит дозволяє визначити, наскільки ефективним є поточний захист корпоративної мережі і які загрози залишаються непоміченими. Постачальник послуги гарантує, що при реалізації рекомендованих в звіті CTAP заходів інформаційна безпека організації на рівні мережі буде відповідати кращим світовим практикам. Маючи можливість провести глибокий аналіз існуючих або можливих загроз, клієнти отримують чітку оцінку ризиків для їх конкретної мережевої інфраструктури та дізнаються, які дії потрібно зробити в першу чергу, щоб знизити ризики й захистити критично важливі активи.

Особливо важливим є внутрішній аудит ІБ підприємства, так як у будь-якої компанії є комерційна таємниця - інформація, яка, потрапляючи в чужі руки, позбавляє компанію переваги на ринку або в своєму сегменті. Є кілька основних видів інформаційних активів, які слід захищати: це власне інформація, інфраструктура, персонал, імідж та репутація компанії. Відповідно, внутрішні загрози ІБ - це можливі дії співробітників з інформаційними активами, умисні або ні, які можуть мати негативні наслідки для компанії. До таких дій відносяться, наприклад, передача інформації тим, від кого хотілося б її приховати, - зловмисникам або конкурентам, шахрайські дії з грошима компанії, або реалізація товару в свою користь.

Для реалізації внутнішнього аудиту існують системи моніторингу дій користувачів, наприклад StaffCop Enterprise - це програма, яка дозволяє контролювати інформаційний обмін та стан інформаційних ресурсів [4]. З її допомогою можна самостійно провести аудит внутрішньої інформаційної безпеки, отримати статистику вразливостей, а також повну інформацію про інциденти. Система дозволяє отримати найрізномані дані та представити їх у вигляді, зручному для аналізу. StaffCop Enterprise має клієнт-серверну архітектуру, тобто складається з серверної частини, яка розміщується у клієнта, та програм-агентів, які встановлюються на комп'ютерах користувачів і збирають інформацію про їхні дії. Інформація обробляється в серверній частині. Повнота збору даних про той чи інший користувача залежить від налаштувань.

Під необхідність налаштування системи, компанія-розробник пропонує клієнтам тест, який можна заповнити письмово або відповісти на питання усно. Це допоможе адаптувати систему під специфіку організації й необхідні завдання. Після розгортання програми та проведення налаштувань система починає збирати інформацію. Сигнали про інциденти надходять на комп'ютер відповідального співробітника або керівника негайно, інша інформація

формується в звіти. При необхідності можна сформувати звіт будь-якої структури, використовуючи зібрану інформацію. Інформація в StaffCop Enterprise структурується за трьома основними напрямками: ІБ, облік робочого часу та адміністрування робочих місць.

Функції моніторингу та блокувань StaffCop Enterprise реалізують превентивну функцію захисту інформації, реалізовуючи наступні можливості:

- контроль присутності на робочому місці;
- логування входу і виходу з системи;
- облік робочого часу;
- реєстрація всіх операцій з файлами;
- створення тіньових копій файлів, що передаються за межі компанії;
- відстеження завантаження файлів в хмарні сховища;
- моніторинг комунікацій співробітників;
- моніторинг електронної пошти по протоколам POP3, IMAP, SMTP;
- перехоплення листів і вкладень через веб-сервіси електронної пошти;
- реєстрація листування в інтернет-месенджерах Skype, ICQ, Jabber;
- реєстрація фактів дзвінків, їх тривалості і архівація SMS в SIP-телефонії;
- реєстрація підключень та блокування USB-пристроїв із категоризацією за класами пристроїв;
- обмеження запису на USB режимом «тільки читання»;
- моніторинг та блокування мережевої активності;
- факти відвідування веб-сайтів та час, проведений на них;
- реєстрація запитів до популярних пошукових систем;
- реєстрація всіх мережевих підключень (програма, ір-адреса, порт);
- факти встановлення та видалення додатків;
- блокування запуску додатків по спискам доступу;
- аудіовізуальний моніторинг співробітників та їхніх комп'ютерів;
- детектор аномалій поведінки користувачів, система сповіщення про інциденти та інші можливості [5].

Система StaffCop Enterprise була розроблена з урахуванням запитів внутрішнбого аудиту ІБ, та повністю відповідає функціональним вимогам по виявленню, аналізу і розслідування інцидентів інформаційної безпеки. Особливістю системи є контроль з командного рядка GNU / Linux, що дозволяє реєструвати всі дії адміністраторів на робочих станціях і серверах з встановленим агентом StaffCop. Така функція розширює список співробітників, які можуть перебувати під наглядом. Перевагою також є можливість перегляду картки співробітника, яка консолідує всю інформацію по певному користувачеві в одному місці.

Окремим випадком аудиту ІБ є тестування на проникнення, або пентестинг. Пентестинг дозволяє в досить короткі терміни об'єктивно оцінити реальний рівень захищеності інформаційних активів організації в умовах сучасного стану способів несанкціонованого доступу до інформації. Головною метою тестування на проникнення є виявлення вразливостей, які можуть бути успішно використані зловмисником. Оцінка захищеності забезпечується шляхом моделювання атак потенційних зловмисників а також пошуком вразливостей системи захисту з їх подальшою експлуатацією. У порівнянні з традиційним аудитом ІБ, основною відмінною рисою тесту на проникнення є: менша глибина охоплення інформаційної інфраструктури організації; велика деталізація знайдених вразливостей; більш точна оцінка ризиків ІБ, заснована на результатах реалізації знайдених вразливостей; велика вірогідність результатів аудиту в порівнянні з класичними методами аудиту, такими як заповнення анкет або опитування співробітників.

Тестування на проникнення дозволяє здійснити оцінку більшої кількості процесів ІБ, ніж інструментальний аудит, та може бути реалізовано з допомогою різноманітних програм, цілих систем або спеціалізованих дистрибутивів ОС (наприклад, Kali Linux).

Висновки відповідно до статті. Отже, основна мета аудиту ІБ полягає в отриманні найбільш повної та об'єктивної оцінки захищеності інформаційної системи, локалізуванні наявних проблем та розробці ефективної програми побудови системи забезпечення ІБ організації. До основних задач аудиту, вирішення яких можна автоматизувати з допомогою програмних додатків, відносятся саме задачі реалізації компонентів системи управління ІБ. Також у межах аудиту ІБ або окремим проєктом може бути проведено тестування на проникнення, або пентестинг, що дозволяє перевірити здатність інформаційної системи компанії протистояти спробам проникнення в мережу й неправомірного впливу на інформаційні ресурси. Беручи до уваги цілі описаних завдань, можна видиліти таку класифікацію об'єктів дослідження з відповідними прикладами:

– комплексні програми оцінки кіберзагроз в рамках мережі, які надають звіт про стан корпоративної мережі, який охоплює ключові загрози ІБ та включає дані про продуктивність і ефективність. Подібні системи дозволяють визначити потенційно вразливі місця і скоригувати політику безпеки організації до настання інцидентів безпеки (Fortinet Cyber Threat Assessment Program);

– комплексні системи моніторингу дій користувачів, які дозволяють провести внутрішній аудит ІБ, що дозволяє визначити слабкі місця системи захисту інформації та оцінити картину інформаційних потоків на підприємстві (StaffCop Enterprice);

– програми забезпечення тестування на проникнення на різних його етапах, та мережеві сканери безпеки, зокрема системи виявлення несанкціонованого доступу (Network Intrusion Detection System), які використовуються для фіксації шкідливого трафіку (NMap, XSpider, Snort, Wireshark);

– засоби розробки та впровадження політик безпеки, які дозволяють проводити розробку політик на основі готових шаблонів, організовувати процеси обговорення, розповсюдження та публікації політик безпеки, а також контролювати інформованість співробітників організації в питаннях ІБ (RUSecure Security Online Support Evaluation);

– програмні засоби для аналізу ризиків ІБ, які дозволяють здійснювати як кількісний, так і якісний аналіз ризиків, а також містять засоби генерації звітів і формування планів обробки ризиків (RA2, MSAT, vsRisk).

Список використаних джерел

1. Попович О. В., Войновська К. О. Особливості аудиту інформаційної безпеки банку при роботі з електронними грошима. *Формування ринкових відносин в Україні*. 2014. № 12. С. 127-130.

2. Fortinet Cyber Threat Assessment. *Fortinet*. URL: https://www.fortinet.com/offers/cyber-threat-assessment.

3. Next-Generation Firewall (NGFW). *Fortinet*. URL: https://www.fortinet.com/products/next-generation-firewall.

4. StaffCop. URL: https://www.staffcop.ru.

5. Обеспечение информационной безопасности. URL: https://www.staffcop.ru/information-security.

References

1. Popovych, O. V., Voinovska, K. O. (2014). Osoblyvosti audytu informatsiinoi bezpeky banku pry roboti z elektronnymy hroshyma [Features of the bank's information security audit when working with electronic money]. *Formuvannia rynkovykh vidnosyn v Ukraini – Formation of market relations in Ukraine*, 12, 127-130 [in Ukrainian].

2. Fortinet Cyber Threat Assessment. *Fortinet*. Retrieved from https://www.fortinet.com/offers/cyber-threat-assessment.

3. Next-Generation Firewall (NGFW). *Fortinet*. Retrieved from https://www.fortinet.com/products/next-generation-firewall.

4. StaffCop. Retrieved from https://www.staffcop.ru.

5. *Obespechenie informatsionnoi bezopasnosti [Information security]*. Retrieved from https://www.staffcop.ru/information-security.

UDC 519.9:004.681

Yuliia Tkach, Mykhailo Shelest, Lesya Chernysh, Svitlana Lytvyn, Artur Bryhynets

ANALYSIS OF INFORMATION SECURITY AUDIT SUPPORT SYSTEMS

Urgency of the research. *In order to ensure the required level of information security at the enterprise it is necessary to regularly conduct security audits of information systems, so the analysis of this process is an urgent task in the field of cybersecurity.*

Target setting. *Currently, there is no dedicated classification, as well as analysis of the parameters of such systems with their subsequent comparison. That is, there is no systematization of data on IS audit support systems, which should allow specialists to make a simpler and more balanced choice of tool for a comprehensive audit, or audit of the information system at a separate stage.*

Actual scientific researches and issues analysis. *Work of many scientists is devoted to the study and systematization of information on the audit and management of information security incidents in Ukraine, but the issues of various types of information security audit support systems have received insufficient attention from Ukrainian scientists.*

Uninvestigated parts of general matters defining. *Despite numerous studies in the field of information security, the classification of research objects during the audit of the enterprise IS has not been proposed yet, and the audit process itself has not been sufficiently analyzed.*

The research objective. *An urgent solution to these problems is the use of various software solutions that greatly facilitate a systematic audit of information security at most of its stages, thus saving enterprise resources.*

The statement of basic materials. *The most complete analysis deserves comprehensive programs and systems that cover the widest range of opportunities to support IS audit. More specialized applications deserve research, depending on the tools and feasibility of the IS audit. Taking into account the objectives of the described tasks, the following classification of research objects can be highlighted with relevant examples: comprehensive cyber threat assessment programs within the network, which provide a report on the state of the corporate network, covering key IS threats and including performance and efficiency data. Such systems allow you to identify potential vulnerabilities and adjust the organization's security policy before security incidents (Fortinet Cyber Threat Assessment Program); comprehensive systems for monitoring user actions, which allow for internal audit of IS, which allows to identify weaknesses in the information security system and assess the picture of information flows in the enterprise (StaffCop Enterprice); intrusion testing programs and network security scanners, including the Network Intrusion Detection System, which are used to detect malicious traffic (NMap, XSpider, Snort, Wireshark); security policy development and implementation tools that allow policy development based on ready-made templates, organize processes of discussion, dissemination and publication of security policies, as well as control the awareness of employees of the organization in matters of IS (RUSecure Security Online Support Evaluation); software for IS risk analysis, which allows for both quantitative and qualitative risk analysis, as well as means for generating reports and forming risk treatment plans (RA2, MSAT, vsRisk).*

Conclusions. *The main purpose of IS audit is to obtain the most complete and objective assessment of the security of the information system, localization of existing problems and development of an effective program for building an IS security system of the organization. The main tasks of the audit, the solution of which can be automated with the help of software applications, are the tasks of implementing the components of the IS management system. Penetration testing or pentesting can also be performed as part of an IS audit or a separate project, which allows to check the ability of the company's information system to resist attempts to penetrate the network and improper influence on information resources.*

Keywords*: information security; information security audit; SMIB; IS incident management; pentesting; risk analysis; information protection.*

References: 5.

Ткач Юлія Миколаївна – доктор педагогічних наук, доцент, доцент, завідувачка кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Tkach Yulia – Doctor of Pedagogical Sciences, Associate Professor, Associate Professor, Head of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: tkachym79@gmail.com
ORCID: http://orcid.org/0000-0002-8565-0525

Шелест Михайло Євгенович – доктор технічних наук, професор, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Shelest Mykhailo– Doctor of Technical Science, Professor, Professor of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mishel3141@gmail.com
ORCID: https:// orcid.org/ 0000-0003-1090-0371
SCOPUS Author ID: 57211429755

Черниш Леся Григоріївна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Chernysh Lesia – PhD in Technical science, Associate Professor, Associate Professor of Department of Cybersecurity and Mathematical Simulation, , Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).

E-mail: lg4@ukr.net
ORCID: http://orcid.org/0000-0001-7446-1684

Литвин Світлана Володимирівна – кандидат педагогічних наук, доцент, завідувач кафедри іноземних мов професійного спрямування, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Lytvyn Svitlana – PhD in Pedagogical Science, Associate Professor, Head of Department of Foreign Languages for Specific Purposes, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: xpower777@gmail.com
ORCID: https:// orcid.org/ 0000-0002-0530-1828
Researcher ID: H-5712-2018

Бригинець Артур Анатолійович – магістрант кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Chernysh Lesia – PhD in Technical science, Associate Professor, Associate Professor of Department of Cybersecurity and Mathematical Simulation, , Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: is.steel.97@gmail.com
ORCID: http://orcid.org/0000-0002-0235-545X