

РОЛЬ ЛЮДСЬКОГО ФАКТОРА ТА ІНЖЕНЕРНО-ПСИХОЛОГІЧНИХ ЗАХОДІВ У КСЗІ: АНАЛІЗ СУЧАСНИХ МОДЕЛЕЙ ПОВЕДІНКОВОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У тезах розглядається роль людського фактору та інженерно-психологічних заходів у комплексних системах захисту інформації (КСЗІ). Проведено аналіз сучасних міжнародних моделей поведінкової безпеки, включаючи NIST SP 800-50(r1), NIST CSF 2.0 та ISO/IEC 27002, та їх порівняння з українськими нормативними документами (НД ТЗІ, ДСТУ). Виявлено, що міжнародні стандарти забезпечують системний та комплексний підхід до навчання персоналу, оцінки поведінки та інтеграції психологічних аспектів, тоді як українські нормативи переважно орієнтовані на формальні організаційно-технічні заходи. На основі аналізу запропоновано рекомендації щодо інтеграції міжнародних практик у КСЗІ українських організацій для підвищення ефективності захисту інформації з урахуванням людського фактору.

Ключові слова: комплексна система захисту інформації, людський фактор, інженерно-психологічні заходи, поведінкова безпека, NIST SP 800-50, NIST CSF 2.0, ISO/IEC 27002, НД ТЗІ, ДСТУ.

Abstract

The article examines the role of the human factor and socio-psychological measures in comprehensive information security systems (CISS). A review of current international models of behavioral security, including NIST SP 800-50(r1), NIST CSF 2.0, and ISO/IEC 27002, is conducted and compared with Ukrainian regulatory documents (ND TZI, DSTU). It was found that international standards provide a more systematic and comprehensive approach to personnel training, behavior assessment, and integration of psychological aspects, while Ukrainian regulations primarily focus on formal organizational and technical measures. Based on the analysis, recommendations are proposed for integrating international practices into Ukrainian CISS to enhance the effectiveness of information protection considering the human factor.

Keywords: comprehensive information security system, human factor, socio-psychological measures, behavioral security, NIST SP 800-50, NIST CSF 2.0, ISO/IEC 27002, ND TZI, DSTU.

Вступ

У сучасному суспільстві інформаційні системи стають дедалі більш критичними – для бізнесу, державних установ, критичної інфраструктури. Водночас, технологічний захист (мережеві рішення, шифрування, технічні засоби) вже не є достатнім: велика частина інцидентів пов'язана з людським фактором – помилками, недбалістю, соціальною інженерією, недостатньою обізнаністю користувачів. Це робить психологічні й поведінкові аспекти безпеки не менш важливими за технічні.

З огляду на це, стає актуальним підхід до безпеки як до комплексної системи, що поєднує не лише організаційні та технічні, але й інженерно-психологічні заходи, спрямовані на формування безпечної поведінки працівників, культуру безпеки, постійне навчання та управління ризиками, пов'язаними з поведінкою.

Метою цих тез є аналіз сучасних моделей поведінкової безпеки (behavioral security / cybersecurity behaviour), які застосовуються чи пропонуються на міжнародному рівні, та оцінка їх придатності в контексті комплексних систем захисту інформації (КСЗІ)

Результати дослідження

Людський фактор залишається однією з провідних причин інцидентів безпеки в інформаційних системах. За результатами щорічного звіту Verizon – 2024 Data Breach Investigations Report (DBIR 2024), близько 68 % підтверджених витоків чи порушень безпеки пов'язані з “не-злочинним людським елементом” – тобто з помилками чи діями користувачів, які не були обумовлені технічними вразливостями, а часто – соціальною інженерією або неправильним поводженням з інформацією [1].

Серед найпоширеніших різновидів загроз, зумовлених людським фактором, – соціальна інженерія, зокрема фішинг, pretexting, імпровізовані атаки через “людський контакт”. DBIR 2024 відзначає, що в межах подій із соціальною інженерією лідируючими залишаються фішинг і підроблені листи: 73 %

інцидентів у цій категорії спричинені email-фішингом або pretexting'ом [1].

Соціальна інженерія використовує людську недбалість, неухважність, брак кіберобізнаності або відсутність сумніву/підтвердження – на шкоду безпеці. У звіті наводиться також, що під час деяких симуляцій phishing-атак приблизно 20 % користувачів виявляють і повідомляють про підозрілі листи, тоді як 11 % із тих, хто натиснув, після цього повідомляли про інцидент – що свідчить про те, що навіть при частковій обізнаності небезпека лишається значною [2].

Ще одним важливим типом загроз є ненавмисні помилки користувачів – неправильне налаштування систем, передчасне/невірне надання доступів, відправка чутливої інформації не тим адресатам, зберігання паролів у небезпечному вигляді тощо. Такі випадки часто класифікуються як “miscellaneous errors” або “human error” в DBIR [2].

Ці помилки становлять суттєву загрозу навіть у добре захищених системах – коли технічні механізми налаштовані правильно, але користувачі нехтують політиками безпеки або діють необачно. Таким чином, надійні технічні заходи не усувають ризик повністю, якщо не враховувати поведінковий компонент.

Додатково, сучасні дослідження підкреслюють, що на поведінку користувачів впливають не лише знання чи навички, але й контекстуальні змінні: корпоративна культура безпеки, тип організації, індустрія, попередній досвід, загальний рівень обізнаності та безпеки, соціальна й національна культура. Наприклад, у недавньому дослідженні Individual and Contextual Variables of Cyber Security Behaviour (2024) показано, що як індивідуальні ознаки (вік, досвід, знання), так і контекстуальні (галузь, культура організації, національні особливості) статистично значимо впливають на ймовірність небезпечної поведінки [3].

Це означає, що боротьба з загрозами, зумовленими людським фактором, не може зводитися тільки до разової інструктажу чи політик. Навпаки – потрібен системний підхід, який враховує людські, організаційні й контекстуальні чинники, що впливають на поведінку.

У сфері формування безпечної поведінки користувачів застосовують низку теоретичних і практичних моделей, спрямованих на пояснення мотивації, оцінку ризиків людського фактора та оптимізацію заходів впливу. Розглянемо детально чотири підходи, які мають наукове обґрунтування, активно застосовуються в інформаційній безпеці та демонструють сумісність із побудовою КСЗІ.

Protection Motivation Theory – психологічна теорія, яка пояснює, як люди ухвалюють рішення щодо захисту себе від загроз. У контексті кібербезпеки PMT застосовується для моделювання поведінки користувачів, зокрема їх намірів виконувати безпекові заходи [4].

PMT основними компонентами є:

- Оцінка загрози – сприйняття вразливості (how likely), і серйозності наслідків (how bad).
- Оцінка здібності впливати (coping appraisal) – віра у власну здатність виконати поведінку (self-efficacy), віра в ефективність заходів (response efficacy), а також урахування витрат на реалізацію (costs).

Багато досліджень показали, що PMT добре пояснює мотивацію дотримуватися політик безпеки. Наприклад, у дослідженні серед працівників державного сектору було з'ясовано, що елементи PMT (особливо self-efficacy та оцінка загрози) корелюють із реальними діями, спрямованими на безпеку. Нещодавнє дослідження (2024) застосувало PMT для розробки “nudging-підходів” (підштовхування користувачів) – коли після повідомлення про порушення безпеки (наприклад, зламаний пароль) отримувач отримував як “threat appeal” (інформацію про ризик), так і “coping appeal” (чіткі інструкції, як змінити пароль). Хоч ефект був невеликим, дослідники констатували, що мотиваційні підходи на базі PMT можуть підвищувати шанси змінити поведінку [5].

SeBIS – стандартизована психометрична шкала, розроблена для вимірювання намірів користувачів дотримуватися “хороших” практик безпеки під час роботи з комп'ютером [6].

Оригінальна валідація SeBIS показала, що високі результати за відповідними підшкалами корелюють з реальною поведінкою: наприклад, користувачі з високим балом за “awareness” краще впізнавали фішингові сайти; високий бал за “passwords” – створювали більш стійкі паролі; “updating” – частіше оновлювали ПЗ; “securement” – ставили блокування на пристрої [6]. Завдяки таким властивостям SeBIS є надійним інструментом для оцінки загального “рівня поведінкової безпеки” серед персоналу, порівняння різних груп (відділів, ролей), вимірювання змін у поведінці після впровадження тренінгів або політик та кількісного аудиту поведінкових аспектів у КСЗІ. Таким чином, SeBIS може слугувати “метрикою” для інженерно-психологічних заходів – дає змогу об'єктивно оцінити, наскільки користувачі готові або вже дотримуються базових безпекових практик.

Окрім індивідуальних мотивів і намірів, значну роль у формуванні безпечної поведінки відіграє організаційна культура, контекст роботи, політики і підтримка. В кількох дослідженнях підкреслюється, що навіть якісні індивідуальні наміри можуть “провалюватися”, якщо контекст не підтримує безпечну поведінку – наприклад, відсутність процедури оновлення, незручні політики, тиск на швидкість

виконання завдань, відсутність заохочень [7].

Один із підходів до інтеграції контексту – поєднання теорій поведінки: Theory of Planned Behavior (TPB), нейтралізаційних теорій (Neutralization Theory) та PMT – як це зроблено в інтегрованій моделі комплаєнсу з політиками інформаційної безпеки. Така модель дозволяє враховувати: ставлення до політик, вплив соціальних норм, самооцінку здатності виконувати вимоги, а також можливість психологічного “виправдання” небезпечної поведінки (neutralization) [7].

Сучасні дослідження все частіше показують, що безпечна поведінка залежить від поєднання індивідуальних і контекстуальних змінних – і ці змінні мають бути враховані при проєктуванні КСЗІ [7].

Оригінальний підхід до управління людським фактором – комбінування моделей мотивації (PMT), психометричних вимірювань (SeBIS), контекстуальних/організаційних факторів (TPB + neutralization / культура безпеки), а також регулярного оцінювання поведінки – дає змогу побудувати системну, адаптивну поведінкову стратегію.

Наприклад, сучасні дослідження (2024) застосовують PMT для створення “nudging-інтервенцій” (нагадувань, сповіщень, поєднаних із інструкціями), що стимулюють зміну поведінки – зокрема зміни паролів після попередніх порушень [5]. Психометричні інструменти (SeBIS) можуть слугувати для моніторингу: наскільки дії користувачів відповідають безпечним практикам, наскільки політики та тренінги змінили поведінку, чи зменшилась “вразливість” персоналу.

Такий інтегрований підхід робить інформаційну безпеку не лише технічним чи адміністративним завданням, а комплексним – з урахуванням людини, її мотивацій, поведінки, контексту та системних умов. Саме це відповідає концепції КСЗІ, в якій інженерно-психологічні заходи мають бути невід’ємною частиною загального захисту.

Розглянемо детально ключові критерії, які відображають підходи до організації людського фактора та поведінкових аспектів безпеки в різних стандартах і нормативних документах в таблиці 1.

Таблиця 1 – Порівняння міжнародних стандартів і українських нормативів щодо інженерно-психологічних заходів у КСЗІ

Критерій	NIST SP 800-50(r1)	NIST CSF 2.0	ISO/IEC 27002	НД ТЗІ / ДСТУ
Основна мета	Організація програм навчання та підвищення обізнаності користувачів щодо інформаційної безпеки; оцінка ефективності навчання	Рамкове управління кіберризиками; включення людського фактора через функцію «Protect», але без деталізації програм навчання	Впровадження стандартів організаційної безпеки, визначення ролей і обов’язків, навчання та підвищення обізнаності	Забезпечення формальних організаційно-технічних заходів; обов’язкові інструктажі, контрольні процедури, обмежене охоплення психологічного аспекту
Підхід до людського фактора	Орієнтований на поведінку користувача: навчальні модулі, симуляції загроз, оцінка реакцій	Включає навчання та підвищення обізнаності як частину управління ризиками; деталізація програм залишена організації	Систематизація ролей, обов’язків, політик; інтеграція поведінкових аспектів через формалізовані процеси	Формальний підхід до навчання та інструктажів; психологічні та мотиваційні аспекти фактично не враховуються
Методи оцінки поведінки	Опитування, тести, симуляції фішингових атак, оцінка поведінки користувача	Моніторинг виконання політик, тестування, KPI без конкретних методик	Внутрішній аудит, перевірка знань, оцінка дотримання політик	Періодичні інструктажі, перевірка дотримання процедур, формальні контрольні заходи
Рівень деталізації	Високий: поетапне планування програм навчання, визначення цільових груп, методи оцінки	Середній: рамкова структура, організація визначає конкретні методи	Високий: конкретні вимоги до процесів, ролей, навчання	Середній: формальні вимоги до процедур і контролю, без детальної роботи з поведінкою користувача

Продовження табл.1

Підхід до інтеграції	Інтеграція мотиваційних і поведінкових методик у навчальні програми	Інтеграція навчання в управління ризиками та процеси організації	Інтеграція політик, ролей та процедур у систему безпеки	Впровадження обов'язкових заходів контролю та навчання без адаптації під поведінкові аспекти користувача
----------------------	---	--	---	--

NIST SP 800-50(r1) спрямований на організацію програм навчання і підвищення обізнаності персоналу у сфері інформаційної безпеки. Документ надає детальні рекомендації щодо структури навчальних програм, визначення цільових груп користувачів, розробки навчальних модулів і оцінки їх ефективності. Особливий акцент робиться на інтеграції навчання з реальними загрозами, включно з фішинговими атаками та іншими соціально-інженерними методами. Такий підхід дозволяє не лише формально ознайомити співробітників з політиками безпеки, а й впливати на їх реальну поведінку, що є критично важливим для комплексної системи захисту інформації. Документ застосовує орієнтований на людину підхід. Програми навчання розробляються з урахуванням поведінки користувача, сприйняття загроз, здатності виконувати безпечні дії та реальної поведінки під час симуляцій атак. Це дозволяє підвищити ефективність заходів з психологічного та поведінкового аспекту, інтегруючи їх у комплексну систему захисту [8].

У NIST SP 800-50(r1) для оцінки ефективності навчання передбачено використання опитувань, тестів, симуляцій фішингових атак та інших методів, що дозволяють оцінити реальну поведінку користувачів. Це забезпечує безпосередній зворотний зв'язок та коригування навчальних програм відповідно до виявлених слабких місць. Документ відрізняється високим рівнем деталізації: документ містить поетапне планування навчальних програм, визначення цільових груп, розробку методів навчання та оцінки ефективності. NIST SP 800-50(r1) інтегрує мотиваційні і поведінкові методики безпосередньо у програми навчання, забезпечуючи поєднання теоретичних знань і практичних навичок [8].

NIST CSF 2.0 надає рамковий підхід до управління кіберризиками. У функції «Protect» навчання і підвищення обізнаності персоналу включені як одна зі складових захисту, проте документ не деталізує конкретні програми навчання чи методики оцінки ефективності. Це дозволяє організаціям самостійно розробляти і адаптувати програми під свої потреби, враховуючи специфіку ризиків і структуру організації. NIST CSF 2.0 враховує людський фактор на стратегічному рівні: навчання та підвищення обізнаності є частиною управління ризиками, проте конкретні методики залишаються на розсуд організації. Це надає гнучкість, але потребує додаткового опрацювання для впровадження ефективних поведінкових інтервенцій. NIST CSF 2.0 пропонує моніторинг виконання політик, використання KPI та тестування персоналу. Методи оцінки залишаються адаптивними, що надає організації можливість самостійно обирати інструменти контролю та оцінки поведінки. NIST CSF 2.0 має середній рівень деталізації: рамкова структура не регламентує конкретні навчальні модулі, залишаючи це на розсуд організації. NIST CSF 2.0 дозволяє організації інтегрувати навчання у процеси управління ризиками та інші функції безпеки [9].

ISO/IEC 27002 встановлює стандартизовані принципи та правила організації безпеки, включно з навчанням і підвищенням обізнаності персоналу. Стандарт підкреслює необхідність визначення ролей і обов'язків співробітників, що дозволяє формалізувати відповідальність за дотримання політик безпеки. ISO/IEC 27002 систематизує ролі та обов'язки персоналу, включає вимоги щодо навчання і підвищення обізнаності, що забезпечує формалізовану інтеграцію поведінкових аспектів у безпекові процеси організації. Стандарт дозволяє організаціям планувати навчальні заходи на основі ролей та рівня доступу співробітників до інформаційних ресурсів. ISO/IEC 27002 передбачає регулярний внутрішній аудит та перевірку знань співробітників, що дозволяє оцінити дотримання ними політик та процедур. Такий підхід формалізує оцінку поведінки та забезпечує стандартизовану основу для контролю. ISO/IEC 27002 забезпечує високий рівень деталізації щодо процесів, ролей, обов'язків та організаційних процедур, що дозволяє інтегрувати поведінкові аспекти в систему безпеки. ISO/IEC 27002 забезпечує інтеграцію політик, ролей і процедур у систему безпеки, формалізуючи поведінкові аспекти [10].

Українські нормативні документи (НД ТЗІ, ДСТУ) орієнтовані на забезпечення формальних організаційно-технічних заходів, включаючи обов'язкові інструктажі та контрольні процедури. Психологічні аспекти поведінки та мотивації персоналу практично не враховуються, що обмежує їх

застосування для впливу на реальну поведінку користувачів. НД ТЗІ і ДСТУ зосереджені на формальних процедурах проведення інструктажів та контролю дотримання правил безпеки. Психологічні та мотиваційні аспекти людського фактора не деталізуються, що знижує потенційну ефективність заходів щодо зміни поведінки персоналу. НД ТЗІ та ДСТУ обмежуються проведенням періодичних інструктажів і перевіркою дотримання процедур. Методи оцінки не включають психометричних або мотиваційних компонентів і, відповідно, менш ефективні для впливу на поведінку користувачів. НД ТЗІ і ДСТУ забезпечують середній рівень деталізації: основна увага приділяється формальним процедурам, інструктажам та контролю, без глибокого аналізу психологічних і поведінкових факторів. НД ТЗІ і ДСТУ зосереджені на формальних заходах контролю та навчання, без адаптації до психологічних і поведінкових особливостей користувачів, що обмежує ефективність впливу на поведінку персоналу.

НД ТЗІ 3.7-003-2005 встановлює порядок проведення робіт зі створення комплексної системи захисту інформації (КСЗІ) в інформаційно-телекомунікаційних системах і визначає повний цикл процедур: від обстеження об'єкта до атестації КСЗІ. Документ надає формалізований процес побудови системи захисту, орієнтований передусім на забезпечення відповідності технічних і організаційних рішень вимогам державних нормативів. Він визначає склад робіт, документації та відповідальних осіб, але не деталізує психологічні чи поведінкові аспекти роботи.

Методи контролю й оцінки поведінки в НД ТЗІ 3.7-003-2005 зводяться до перевірки дотримання встановлених інструкцій, ведення журналів, нагляду за режимом доступу та періодичного проведення інструктажів. Документ не передбачає кількісних показників ефективності, оцінювання компетентностей персоналу, тестування знань, аналізу помилок або застосування психометричних інструментів. Натомість він надає формальні механізми підтвердження виконання процедур, що забезпечує відповідність вимогам, але не гарантує реального впливу на поведінку користувачів.

За рівнем деталізації НД ТЗІ 3.7-003-2005 має нормативно-процедурний характер: він детально описує процес побудови КСЗІ, але практично не деталізує заходи роботи з персоналом з точки зору психології, соціотехнічних ризиків чи поведінкових механізмів. У межах документу навчання персоналу та підтримання режиму безпеки трактується як формальна складова впровадження КСЗІ, що виконується для забезпечення відповідності вимогам держави. НД ТЗІ 3.7-003-2005 забезпечує структурованість і уніфікованість процесів, проте не охоплює сучасних підходів до роботи з людським фактором, які використовуються у міжнародних стандартах. Це створює розрив між технічною відповідністю та реальними поведінковими ризиками, які залишаються поза сферою регуляції [11].

Висновки

Аналіз ролі людського фактора та інженерно-психологічних заходів у комплексних системах захисту інформації засвідчив, що вплив поведінкових чинників на інформаційну безпеку є критично значущим і підтверджується міжнародною статистикою інцидентів. Моделі поведінкової безпеки, такі як Protection Motivation Theory, SeBIS та огляди ENISA, демонструють, що ефективність системи захисту визначається не лише технічним рівнем контролів, а й здатністю організації формувати сталі патерни безпечної поведінки персоналу.

Міжнародні стандарти (NIST SP 800-50(r1), NIST CSF 2.0, ISO/IEC 27002) розглядають навчання, мотивацію, культуру безпеки та оцінку поведінкових ризиків як невід'ємні елементи управління кіберризиками. Вони включають підходи до побудови навчальних програм, використання метрик, аналізу людських помилок та інтеграції поведінкових механізмів у систему контролів. Така орієнтація на психологічні та когнітивні процеси наближає сучасні системи безпеки до соціотехнічної парадигми.

Українські нормативні документи, зокрема НД ТЗІ 3.7-003-2005, забезпечують високий рівень процедурної та організаційної визначеності, але людський фактор у них розглядається переважно через призму формального інструктажу та контролю. Вони не охоплюють психологічні особливості користувачів, не враховують мотиваційні та когнітивні механізми ризиків і не містять інструментів поведінкової оцінки, що створює методологічний розрив порівняно з міжнародними практиками.

Отже, для підвищення ефективності комплексних систем захисту інформації в Україні доцільним є інтегрування сучасних поведінкових та інженерно-психологічних підходів, що базуються на міжнародних моделях і стандартах. Це дозволить оптимізувати навчальні процеси, підвищити рівень усвідомленості загроз, зменшити частоту людських помилок та адаптувати КСЗІ до реальних соціотехнічних умов функціонування організацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Verizon Data Breach Investigations Report: Social Engineering Insights. *dmarcian*. URL: <https://dmarcian.com/verizon-2024-dbir/> (date of access: 07.12.2025).
2. Verizon Sourcing LLC. 2024 Data Breach Investigations Report: Half of the Breaches in EMEA are Internal. *GlobeNewswire News Room*. URL: <https://www.globenewswire.com/de/news-release/2024/05/01/2872903/0/en/2024-Data-Breach-Investigations-Report-Half-of-the-Breaches-in-EMEA-are-Internal.html> (date of access: 07.12.2025).
3. Individual and Contextual Variables of Cyber Security Behaviour -- An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour. *arXiv.org*. URL: <https://arxiv.org/abs/2405.16215> (date of access: 08.12.2025).
4. Determinants of Security Behavior Intention in State-Owned Enterprises: Applying Protection Motivation Theory to Phishing Emails | IIETA. *IIETA | Advancing the World of Information and Engineering*. URL: <https://iieta.org/journals/ijssse/paper/10.18280/ijssse.150304> (date of access: 08.12.2025).
5. Nudging Users to Change Breached Passwords Using the Protection Motivation Theory. *arXiv.org*. URL: <https://arxiv.org/abs/2405.15308> (date of access: 09.12.2025).
6. Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS). *Israeli Research Community Portal*. URL: <https://cris.iucc.ac.il/en/publications/behavior-ever-follows-intention-a-validation-of-the-security-beha-2/> (date of access: 10.12.2025).
7. An Integrative Behavioral Model of Information Security Policy Compliance - PMC. *PMC Home*. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC4058133/> (date of access: 10.12.2025).
8. Wilson M. Withdrawn NIST Technical Series Publication. *NIST Technical Series Publications*. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf> (date of access: 10.12.2025).
9. Cybersecurity Framework. *NIST*. URL: <https://www.nist.gov/cyberframework> (date of access: 10.12.2025).
10. ISO Library - Your Complete ISO Standards Resource. *ISO Library - Comprehensive ISO Standards Guide*. URL: <https://iso-library.com/standard/27002/> (date of access: 11.12.2025).
11. *T3I - інформаційна безпека та захист інформації*. URL: <https://tzi.com.ua/downloads/3.7-003-2005.pdf> (дата звернення: 11.12.2025).

Пінчук Дар'я Олександрівна – студентка групи 1KITC-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Науковий керівник: **Павловський Павло Валерійович** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: prepod@vntu.edu.ua

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Supervisor: **Pavlovsky Pavlo V.** – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: prepod@vntu.edu.ua