КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.13.226242
УДК 004.056.5

Крючкова Лариса Петрівна
доктор технічних наук, професор,
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент,
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Ворохоб Максим Віталійович
викладач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

ПЕРЕДПРОЄКТНІ РІШЕННЯ ЩОДО ПОБУДОВИ СИСТЕМИ АВТОРИЗАЦІЇ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST

Анотація. У цій статті розкрито завдання побудови ефективних рішень задля підвищення рівня кібербзепеки інформаційних систем державного рівня в умовах зброї агресії та потужних кібератак на критичну інфраструктуру. Розроблено описове доповнення моделі загроз безпеки з урахуванням концепції Zero Trust, а також візуалізовано моделі загроз, яка дозволяє визначити потенційні вразливості існуючих рішень щодо побудови підсистем ідентифікації і управління доступом. Визначено вимоги до безконтактного апаратного засобу автентифікації. Побудовано функціональну схему взаємодії компонентів радіочастотної ідентифікації з пасивними електричними коливальними контурами. Створено блок-схему алгоритму роботи системи ідентифікації до апаратного пристрою автентифікації . Визначені функціональні та інженерні рішення щодо побудови безконтактного апаратного засобу автентифікації клієнтів під час доступу до пристроїв системи. Обґрунтовані ескізні рішення щодо побудови стеганографічного протоколу обміну даними в процедурах ідентифікації і управління доступом.

Ключові слова: кібербезпека; інформаційна система; кібератака; критична інфраструктура; модель загроз; автентифікація; ідентифікація; стеганографія; протокол; управління доступом.

ВСТУП

Створення складних систем інформаційної взаємодії та управління типу мережі ситуаційних центрів держави [1] потребує розв’язку низки складних завдань, зокрема, визначення архітектури системи управління інформаційною безпекою та застосовних в ній механізмів захисту інформаційних ресурсів [2]–[4].

Відповідно до вимог нормативних документів [3] вихідними даними для розробки Політики інформаційної безпеки є результати обстеження об’єктів інформатизації та розроблення моделі загроз та моделі порушника. У зв’язку з поширенням технологій хмарних сервісів та аналізом потенційних можливостей порушників безпеки [7], [8]

© Л.П. Крючкова, П.М. Складанний, М.В. Ворохоб, 2023

набувають актуальності дослідження та розробки методів побудови систем захисту інформації з урахуванням положень концепції Zero Trust, інакше — моделі «повної недовіри».

В якості моделі безпеки Zero Trust [9] запропонована відомим аналітиком Дж. Кіндервагом в 2010 році. З того часу ця модель набула значної популярності серед експертів як ефективна концепція забезпечення кібербезпеки.

Аксіомою концепції Zero Trust є відсутність довіри до будь-якого суб'єкта і об'єкта (пристрою) інформаційної системи, навіть якщо вони перебувають у середині контуру безпеки. За суттю, модель передбачає, що для кожного випадку звернення до ресурсу системи всередині або зовні контуру безпеки, кожен користувач або пристрій повинні підтверджувати власні ідентифікаційні дані.

Викладене актуалізує завдання дослідження та побудови ефективних рішень, що підвищують рівень кібербезпеки інформаційних систем державного рівня в умовах збройної агресії та потужних кібератак на критичну інфраструктуру.

МОДЕЛЬ ЗАГРОЗ БЕЗПЕКИ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST

Базовими механізмами захисту інформаційних ресурсів в комп'ютерних системах традиційно є процедури ідентифікації суб'єктів, процесів і об'єктів цих систем, авторизація суб'єктів та управління доступом суб'єктів та процесів до об'єктів згідно з визначеною Політикою безпеки. Належним чином ідентифікована та автентифіковані суб'єкти та процеси отримують на основі правил розмежування доступу право на читання інформації (отримання даних) з певного її носія та/або запис (передачу) деякої інформації на носій, або запуск в системі обчислювального процесу (програми).

В умовах початкового уявлення про порушника інформаційної безпеки переважно (іноді, навіть, виключно) як сторонньої по відношенню до системи особи підсистема авторизації та управління доступом — *IAM* (*Identity & Access Management*) замислювалася як централізований механізм для обмеження доступу до ресурсів системи та контролю за ним на основі надання дозволів користувачам або групам користувачів. Метою функціонування *IAM* спочатку було надання прав, а не контроль, а доступ повністю ґрунтувався на реєстрації в *IAM* умовного імені користувача (логіна) та пароля у поєднанні з членством у групі чи дозволами, що визначають право скористатись тим чи іншим ресурсом.

Пізніше ця модель зазнала різних модифікацій з метою:

- посилення надійності і ефективності процедур ідентифікації і автентифікації, зокрема, шляхом впровадження їх багатофакторної побудови;
- конкретизації повноважень користувачів і менеджменту безпеки, при цьому деталізація рішення щодо умов надання доступу в системі відбувалась централізовано в таких органах управління як служба або інфраструктура ідентифікації.

З часом, як було зазначено раніше, ландшафт вірогідних загроз суттєво змінився, і сьогодні поняття потенційного порушника включає не тільки конкретну особу, а й деякий альянс осіб, які можуть ситуативно або системно діяти для досягнення певної зловмисної мети, що може бути визначена в термінах порушення конфіденційності, цілісності та доступності інформації. Нині нерідко спостерігаються випадки, коли спочатку лояльні до роботодавця співробітники згодом з різних мотив починали діяти на

користь його конкурентів або зловмисників, коли виходячи корисливих спонукань відповідальні особи починають діяти всупереч норм корпоративної етики і моралі для власного збагачення. Застосування для доступу до інформаційних систем мобільних пристроїв, включаючи ноутбуки, планшети, смартфони підвищує ризики їх втрат та крадіжок, що утворює підґрунтя для реалізації несанкціонованого доступу до цих систем завдяки доступу зловмисників до апаратної і програмної платформи, а також критичної інформацій, яка може зберігатись на цьому пристрої.

Зважаючи на те, що *IAM* є ключовим механізмом будь-якої моделі розмежування доступу до ресурсів системи, та виходячи з необхідності його постійного вдосконалення і розвитку для забезпечення спостережності подій в комп'ютерних мережах уявляється доцільним з'ясувати вразливості існуючих рішень щодо побудови цієї системи.

Для цього, на підставі аналізу публікацій та повідомлень у ЗМІ про інциденти та негативні явища в комп'ютерних системах розроблена описове доповнення моделі загроз безпеки з урахуванням концепції Zero Trust (таблиця 1, рис. 1).

Запропонована модель робить більш очевидними потенційні вразливості існуючих рішень щодо побудови підсистем *IAM*:

– одноразова процедура автентифікації може бути використана іншими користувачами або зловмисником. Зокрема, у випадку, якщо процедури ІАУ виконані, а легальний користувач з певних причин залишив робоче місце, подальші дії зловмисника обмежуються лише можливістю входу, контрольовану територію і визначеними для конкретного користувача правами доступу;

Таблиця 1

Часткова модель загроз згідно концепції Zero Trust

Роль	Точка доступу	Небезпечні дії
Відправник (Transmitter)	Власне АРМ або АРМ колеги	Ненавмисні (помилкові)дії *ВІДМОВА* (щодо відправлення) *МАСКАРАД* (видача за іншу особу) *ЗМОВА* (із зловмисником)
Отримувач (Receiver)	Власне АРМ або АРМ колеги	Ненавмисні (помилкові)дії *ВІДМОВА* (щодо отримання) *МОДИФІКАЦІЯ* (отриманого) *ПІДРОБКА* (неіснуючого) *МАСКАРАД* (видача за іншу особу) ЗМОВА (із зловмисником)
Провайдер (Provider)	Робоче місце адміністратора безпеки	Ненавмисні (помилкові)дії ЗМОВА (із зловмисником)
Зловмисник (Interceptor)	Легальне АРМ або власний засіб	ПЕРЕХОПЛЕННЯ (змісту) МОДИФІКАЦІЯ (отриманого) ПІДРОБКА (неіснуючого) МАСКАРАД (як легальний користувач) ПОВТОР (перехопленого)

– відкрито застосовані логіни користувачів можуть бути використані зловмисником для аналізу трафіка в інформаційній мережі, який в певних застосуваннях, навіть без розкриття його змісту, може становити значний інтерес для отримання розвідувальної інформації;
– процедури ідентифікації і автентифікації сприймаються як логічні предикати, що можуть мати значення лише значення «істина» (true) або

«хиба» (false). Насправді, переважна більшість процедур при цьому носить ймовірнісний характер Реальне виконання або не виконання умов авторизації завжди має ймовірнісний характер. Наприклад, користувачі достатньо часто помиляються під час набору реально стійкого паролю, його зчитування з носія може супроводжуватись збоєм або помилкою, біометричні процедури взагалі виконується з певною ймовірністю помилки;

– користувачі, що мають доступ до декількох систем (включаючи власні комп'ютери), зазнають проблеми з надійним збереженням складних стійких паролів, які мають значну кількість букв, цифр та інших символів.

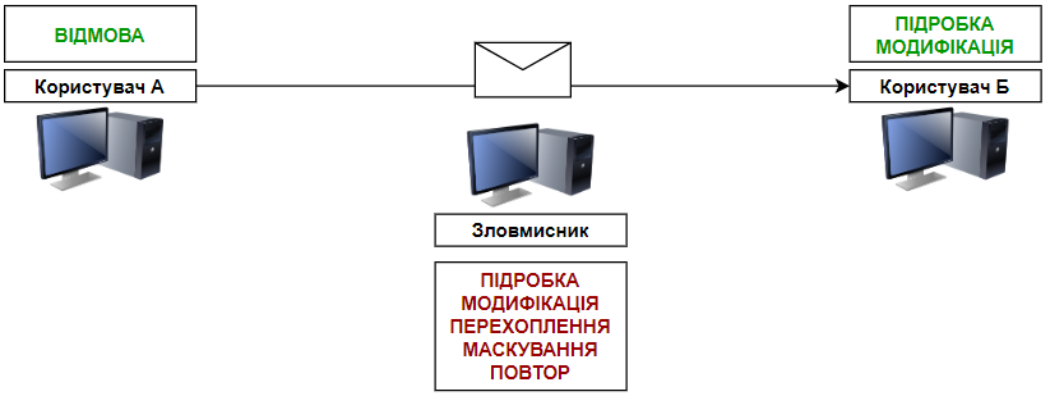

Рис. 1. Візуалізація моделі загроз згідно концепції Zero Trust

Застосування звичайних компактних флеш носіїв для збереження критичної інформації звичайно не покращує безпекову ситуацію, оскільки незахищені носії паролів та інших чутливих даних дуже часто залишаються користувачами системи без дієвого контролю та, іноді, взагалі губляться.

Вартість же захищених носіїв доволі велика, що може суттєво обтяжувати бюджет власника великої інформаційної системи.

З метою покращення безпекової ситуації та нейтралізації існуючої вразливостей доцільно розглянути низку рішень, що можуть бути реалізовані без значних капітальних вкладень:

1. Політикою безпеки повинен бути визначений гранично припустимий час дійсності процедури автентифікації, звернення до більш чутливих даних потребує нової автентифікації. Частота автентифікація суб'єктів інформаційного обміну та використовуваних пристроїв на основі їх облікових даних має бути інструментом реагування на інциденти в системі: у випадку зростання кількості інцидентів в системі припустимий час дії з попередньою автентифікацією повинен скорочуватись.

2. Політика безпеки повинна максимально обмежувати надання доступу до ресурсів, дозволяючи доступ лише до необхідної інформації та пристроям.

3. Джерелом прийняття рішень менеджментом безпеки має бути об'єктивна інформація про стан роботи IAM. З метою аналізу та прийняття рішень щодо проведення тестування або модернізації IAM, додаткових тренінгів з персоналом або обмеження прав доступу до критичних ресурсів певним особам загальна статистика помилок автентифікації кожного учасника інформаційного обміну повинна накопичуватися протягом визначеного проміжку часу (місяць, квартал, рік).

4. Логіни доступу суб'єктів інформаційних відносин повинні зберігатись як службова інформація, а для їх приховування доцільно застосування криптографічних або стеганографічних протоколів.

5. Для підвищення рівня безпеки процедур автентифікації доцільно застосовувати фактори особистості співробітника, які не потребують застосування складних біометричних технологій.

Зокрема, така автентифікація може забезпечуватись шляхом впізнання голосу «диктора», що зачитує визначену на екрані монітора послідовність чисел. При цьому програмний засіб на основі еталонних даних про голос кожного користувача та відомих математичних алгоритмів їх обробки може розраховувати меру належності тестового повідомлення всім потенційним учасникам процедури автентифікації. А це суттєво скоротить кількість бажаючих випробувати свої акторські здібності.

6. Для переключення *IAM* в режим автентифікації доцільно використовувати картки користувачів, що реалізують технології безконтактного підключення, Зокрема, це може бути достатньо проста і ефективна технологія RFID.

ВИЗНАЧЕННЯ ВИМОГ ДО БЕЗКОНТАКТНОГО АПАРАТНОГО ЗАСОБУ АВТЕНТИФІКАЦІЇ

Виходячи з побудованої моделі загроз визначимо основні функціональні та ергономічні вимоги до апаратного пристрою автентифікації (*Hardware Authentication Device — HAD*), з урахуванням системуних вимог до побудови центру кібербезпеки критичної інфраструктури [5], а саме:

- безконтактне підключення до засобів контролю доступу;
- невеликі малогабаритні характеристики;
- малий рівень електроспоживання;
- зручність застосування для автентифікації різних видів доступу, включаючи прохід в приміщення підвищеної безпеки, двофакторна автентифікація користувачів в інформаційній системі тощо;
- можливість багаторазового застосування та перепрограмування параметрів;
- фізичний захист від несанкціонованого доступу до даних, які зберігаються в *HAD*;
- накопичення даних поточної активності в системі, включаючи спроби доступу до ресурсів с порушенням визначених правил, облік фактичного часу доступу до ресурсів системи тощо;
- створення сеансового ключу шифрування для віддаленого доступу до ресурсів. Кожен блок даних, що надсилається одним з учасників освітнього іншому має бути захищений за допомогою коду автентифікації повідомлень MAC;
- шифрування конфіденційних даних за допомогою ключа симетричного алгоритму, який генерується та зберігається в *HAD* без можливості його вилучення. Для розшифрування даних має бути передбачена процедура відновлення ключа (recovery) на основі 2-х ключів з 3-х певної множини ключів, власниками яких є персонал системи;
- формування/перевірка електронного підпису власника *HAD* та перевірка підпису посадових осіб за наявності сертифікату відкритого ключа. Кожен

документ, що зберігається в *HAD*, має бути підписаним його власником та адміністратором безпеки).

Раціональним рішенням реалізації в *HAD* безконтактного методу передачі автентифікаційних даних може бути використання стандартизованих на поточний час радіо інтерфейсів типів *Bluetooth, WiFi, RFID*.

При цьому задача створення *HAD* з усіма переліченими вище елементами полягатиме у виборі серед сукупності можливих такого варіанту системи ідентифікації, який забезпечив би надійну її роботу із заданою якістю при мінімальних капітальних та експлуатаційних витратах.

Найважливішою складовою частиною зазначеної системи ідентифікації є її первинний вимірювальний перетворювач (ПВП). ПВП повинен мати високу швидкодію, бути чутливим до первинного інформативному параметру та забезпечувати стабільність характеристик в умовах впливу дестабілізуючих факторів [10]. Зазначені характеристики тісно взаємопов’язані.

При цьому поліпшення однієї призводить, як правило, до погіршення інших. Так, підвищення точності вимірювання інформативного параметра сприятиме зниженню швидкодії, і навпаки, при підвищенні швидкодії ПВП знижується точність вимірювання. Оскільки точність — це категорія економічна (тобто, чим точніше вимірюється інформативний параметр, тим ефективніше отримана інформація може бути використана, однак вартість її отримання зростає), при створенні системи ідентифікації *HAD* необхідно вирішувати компромісну задачу вибору оптимальних співвідношень усіх, перелічених вище параметрів.

Можливими методами її вирішення є [11]:

- математичне моделювання системи ідентифікації HAD. Його перевага полягає в можливості проведення оцінювання статичних та динамічних характеристик таких систем. Обмеженість обумовлена тим, що ступінь достовірності моделей залежить від практичного та теоретичного досвіду їх розробників;
- формування та дослідження узагальнених показників системи ідентифікації HAD з використанням графоаналітичного методу, методу «прогресуючого еталону» тощо. Перевага цих методів полягає в можливості урахування великої кількості часткових показників єдиною числовою характеристикою — узагальненим показником, що дає можливість достатньо просто проводити порівняльне оцінювання таких систем. Обмеженість пов’язана з тим, що ці методи не враховують деякі економічні та виробничі фактори;
- застосування експертних методів оцінювання, що базуються на використанні узагальненого людського досвіду — «колективної мудрості».

При цьому саме методи експертних оцінок вважаються визначальними при вирішенні складних завдань оцінювання та вибору будь-яких об’єктів, при аналізі та прогнозуванні ситуацій з великою кількістю значимих факторів. Їх застосовують, як правило за умови, що «… вибір, обґрунтування та оцінювання результатів рішень не можуть бути виконані на основі точних розрахунків.

Це забезпечує активну й цілеспрямовану участь фахівців на всіх етапах прийняття рішень, що уможливлює суттєве підвищення їхньої якості й ефективності» [11]. Експертні методи дають можливість більш глибоко вивчити явища, які слабко піддаються вивченню іншими методами, а також виявити найбільш важливе та істотне, не опускаючи тих деталей і взаємозв’язків, без яких не може бути побудована модель досліджуваної проблеми.

Основними недоліками методів є суб'єктивізм думок експертів у відшукуваних оцінках та обмеженість їхніх суджень. Головна перевага зазначених методів, враховуючи незначні вимоги щодо наявності апріорної інформації про об'єкт дослідження, полягає у відносній простоті та зручності застосування для прогнозування практично будь-яких ситуацій.

Головним показником для оцінки якості системи ідентифікації HAD експерти вважають, як правило, достовірність результатів ідентифікації. Вона виражається ймовірністю правильної ідентифікації HAD. Правомірність імовірнісного підходу при оцінці якості системи ідентифікації пояснюється випадковим характером процесів, що відбуваються при ідентифікації, коли внаслідок впливу дестабілізуючих факторів і випадкових зовнішніх збурень змінюються параметри як вимірювальних засобів, так і самих ідентифікаційних ознак HAD. Результати ідентифікації при цьому розглядаються як випадкові події, з певною ймовірністю відповідні реальним ідентифікаційним ознакам HAD.

Зважаючи на викладене найбільш прийнятною для ідентифікації HAD є технологія RFID з індуктивним зв'язком, яка в якості ідентифікаційних ознак використовує пасивні електричні коливальні контури (ПЕКК). Власне сама система ідентифікації HAD має складатися з (рис.2):

- комплекту HAD з носіями ідентифікаційних ознак;
- зчитувачів з приймально-передавальним інтерфейсом для зв'язку з носіями коду HAD, розташованих в зоні ідентифікації;
- додатку, встановленого на комп'ютері (планшеті).

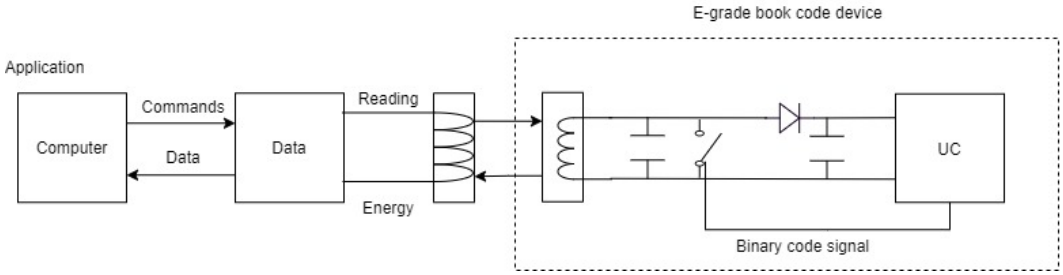

Рис. 2. Функціональна схема взаємодії компонентів RFID з ПЕКК

Завдання зчитувача: активізувати носій коду, внесений в зону ідентифікації; приймати ідентифікаційний номер носія з подальшою передачею за допомогою програмних драйверів до *IAM*.

Первинний вимірювальний перетворювач в технології RFID з індуктивним зв'язком являє собою електричний коливальний контур, налаштований в резонанс на частоту живлючого генератора. Чутливим елементом ПВП є індуктивність, виконана у вигляді рамки. Як інформативний параметр ПВП використовується амплітуда вихідної напруги ПВП.

При попаданні в зону ідентифікації, ПЕКК, частота налаштування якого збігається з частотою електромагнітного поля зчитувача, відбирає енергію цього поля. Таким чином, пасивні RFID мітки з чіпом отримують енергію для функціонування.

Ідентифікаційний код HAD формується шляхом комутації (закорочування) ПЕКК відповідно з присвоєним кодом (так звана навантажувальна модуляція — *load modulation*). Обробку вхідної інформації та вироблення відповідного сигналу забезпечує кремнієвий КсМОП-чіп (чіп КсМОП — чіп комплементарної структури «метал-оксид-напівпровідник»).

Вибір КсМОП — напівпровідникової технології побудови інтегральних мікросхем пояснюється близьким до нуля енергоспоживанням в статичному стані. Схема взаємодії ПВП і ПЕКК представлена на рис. 3.

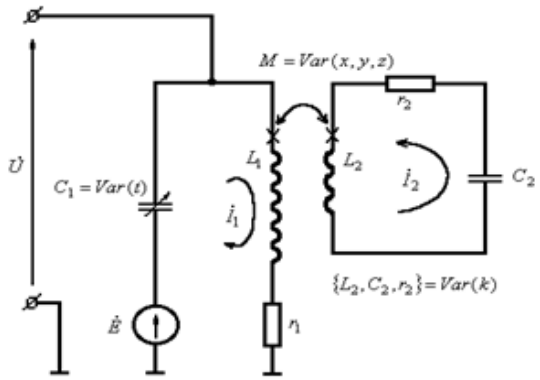

Рис. 3. Схема взаємодії ПВП и ПЕКК:
L_1 — джерело поля; L_1C_1 — контур джерела поля; $\dot{E}$ — генератор напруги, що живить контур джерела поля; L_2C_2 — ПЕКК; $\dot{U}$ — інформативний параметр; M — коефіцієнт взаємної індукції між котушками L_1 и L_2; x, y, z — координати внесення ПЕКК; k — поле значень частот налаштування ПЕКК

Процес взаємодії ПВП з ПЕКК об'єкта може бути поданий [11] у вигляді наступної математичної моделі:

$$\dot{U} = \dot{E}\frac{(r_1 + \frac{w^2M^2}{|z_2|^2}r_2) + j(x_{L_1} - \frac{w^2M^2}{|z_2|^2}x_{2)}}{(r_1 + \frac{w^2M^2}{|z_2|^2}r_2) + j(x_1 - \frac{w^2M^2}{|z_2|^2}x_{2)}} \quad (1)$$

де r_1 та r_2 — власні втрати в контурі джерела поля і ПЕКК;

$Z_1 = r_1 + j(\omega L_1 - \frac{1}{\omega C_1})$ і $Z_2 = r_2 + j(\omega L_2^{\dot{E}} - \frac{1}{\omega C_2})$ — комплексний опір кожного з контурів;

ω — кругова частота джерела э.д.с. E.

Максимальний радіус зчитування R обмежується величиною ближньої зони електромагнітного поля: $R < \lambda / 2\pi$, де λ — довжина хвилі електромагнітного поля, створюваного джерелом поля. Аналіз рівняння (1) показує, що зміна напруги на джерелі поля визначається зміною знаменника.

Збільшення активного опору контуру джерела поля призводить до зменшення напруги на джерелі поля L_1. Отже, по зменшенню напруги на джерелі поля, викликаного збільшенням необоротних втрат енергії, можна судити про наявність на об'єкті ПЕКК, частота налаштування якого збігається з частотою поля (рис. 3).

ПЕКК «спрацьовує», коли залишкове значення інформативного параметра досягає контрольованого рівня. Зона вибору контрольованого рівня інформативного параметра, задається опорним (пороговим) значенням напруги компаратора U_n, обмежується зоною нестабільності початкового значення інформативного параметра ПВП. Системи RFID з індуктивним зв'язком між носієм ідентифікаційного коду і зчитувачем, працюють на частоті нижче 135 кГц або в діапазонах частот 6,78; 13,56 і 27,125 МГц [12], [13].

Блок-схема узагальненого алгоритму ідентифікації HAD представлена на рис. 4.

ISSN 2663 - 4023

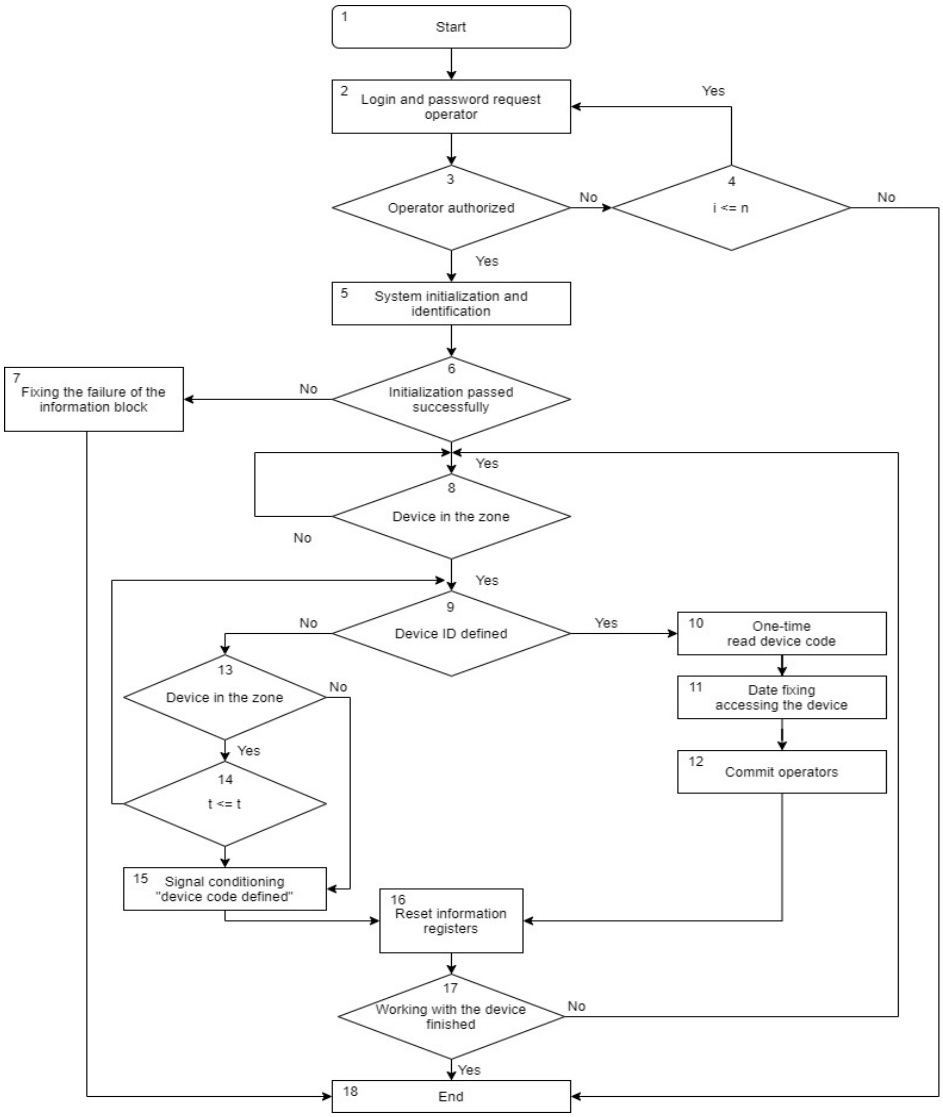

Рис. 4. Блок-схема алгоритму роботи системи ідентифікації HAD

Для підвищення достовірності ідентифікації в зчитувачі застосовується процедура «хитання» частоти генерованого електромагнітного поля між двома граничними значеннями. Коли частота електромагнітного поля точно збігається з частотою настройки ПЕКК носія, виникає виразний перепад інформативного параметра ПП, який достовірно фіксується зчитувачем.

Необхідні для достовірної ідентифікації параметри зчитувача і носія ідентифікаційного коду регламентуються стандартами ISO/IEC 18000 [14]–[16]. При цьому ISO/IEC 18000-2: 2004, наприклад, визначає:

- фізичний рівень, який використовується для зв’язку між зчитувачем і носієм ідентифікаційного коду;
- протокол і команди;
- метод виявлення і зв’язку з одним носієм серед кількох носіїв («антіколлізія»).

Стандарт ISO/IEC 18000-2: 2004 визначає два типи носіїв: Тип A (FDX) і Тип B (HDX). Ці два типи відрізняються тільки своїм фізичним рівнем. Обидва типи підтримують один і той самий протокол захисту від взаємних впливів.

Носії FDX працюють на частоті 125 кГц і постійно отримують живлення від зчитувача, в тому числі під час передачі ідентифікаційного коду від носія до зчитувача. Носії HDX працюють на частоті 134,2 кГц і отримують живлення від зчитувача, за винятком часу передачі ідентифікаційного коду від носія до зчитувача.

Авторизація оператора проводиться з метою виконання вимог політики розмежування доступу.

Ініціалізація системи ідентифікації *HAD* забезпечує приведення програмних і апаратних засобів системи в стан готовності до використання. При внесенні *HAD* в зону ідентифікації системи і успішного визначення коду проводиться фіксація цього коду в системі управління інформаційною безпекою. При цьому фіксуються дата звернення до носія та ім'я оператора.

Після винесення *HAD* із зони зчитування проводиться скидання інформаційних регістрів і система ідентифікації вважається готовою до роботи з наступним *HAD*. У разі невизначення коду *HAD* після певного періоду, $t_{ож}$ системою формується сигнал «код носія не визначений».

СТЕГАНОГРАФІЧНИЙ ПРОТОКОЛ ОБМІНУ ДАНИМИ В ПРОЦЕДУРАХ ІАМ

Побудова системи ІАМ потребує опрацювання питань захисту чутливої інформації під час її передавання через деяке потенційно небезпечне середовище. Основним методом, що забезпечує захист даних при обміні в комп'ютерних системах, є застосування криптографічних протоколів типів SSL, TLS, SET, SSH тощо. Вони поєднують достатню швидкодію з надійним захистом даних. При цьому забезпечується їх конфіденційність і цілісність.

Водночас необхідно зазначити що стандартні криптографічні протоколи іноді можуть використовувати за замовчуванням застаріли криптографічні механізми які вразливі до деяких видів атак [17]–[19]. Також слід звернути увагу на те, що у випадку використання стандартного протоколу основний контроль за ключовою та іншою критичною інформацією забезпечує операційна система комп'ютера, яка може зберігати у власному ядрі дані про застосовані ключі, що не підвищує рівня довіри до системи захисту.

На відміну від криптографічних перетворень стеганографія приховує факт передавання критичної інформації, що фактично є доволі ефективним способом убезпечення конфіденційної інформації [17]–[24].

Цифрової або комп'ютерна стеганографії оперує з поняттям стеганографічної системи (далі — стегосистеми) яка задається наступним рівнянням:

$$\tilde{Q} = \mathcal{F}(Q, k, D), \tag{2}$$

де $D = (d_1, \dots, d_L) \in V_2^L$ — інформаційний вектор — двійковий рядок довжини L; $Q \in \{Q_i,\ i = 1,2, \dots\}$ — двійковий файл з деякої кінцевої їх множини форматів аудіо, зображення тощо. Цей файл зазнає перетворень згідно з правилом — функцією $\mathcal{F}$ на основі інформаційного вектору та з використанням таємного параметру $\bar{k} \in \{k_j,\ j = 1,2, \dots\}$ — ключа стегосистеми.

Файл Q отримав назву пустого контейнера, файл $\tilde{Q}$ — контейнер що містить замаскований інформаційний вектор I та використовується для прихованого передавання цього вектора через незахищене середовище [20]. При цьому сукупність $\langle \mathcal{F}, Q \rangle$ є стеганографічною системою, або коротко — стегосистемою.

Як і загально відомі широкосмугові системи радіозв'язку стеганографічні системи забезпечують ефективне маскування факту передачі деякого повідомлення. Отже властивість стегосистем може бути використана захисту інформаційного обміну в рамках реалізації процедур автентифікації. Таким чином, виходячи з потреби практики можливо відмітити актуальність розробки безпечної стегосистеми.

Загально визнаними критеріями щодо визначення безпеки застосування стегосистеми є надання відповіді на наступні базові питання.

П.1. Чи існує деяка процедура, яка дозволяє стосовно перехопленого контейнера стверджувати, що він пустий?

П.2. Чи можна без знання ключу стегосистеми за оперативне прийнятний час з заданим рівнем надійності з контейнеру вилучити саме то повідомлення, яке в нього було вбудоване?

Очевидно відповіді на ці питання залежать від характеристик функції перетворення та обраних контейнерів.

Для побудови захищеного стеганографічного протоколу перш за все почнемо з визначення функції перетворення $\mathcal{F}$, за допомогою якої встановлюється правило вбудовування інформаційного вектора в стеганографічний контейнер Q.

Логічно вимагати, щоб відповідне правило $\mathcal{F}$ для забезпечення високої швидкості перетворення мало відносно невелику обчислювальну складність та його реалізація програмним засобом була узгоджена з системою команд використаного процесора.

Серед значної кількості таких функцій [20]–[26] вказаній вимогі відповідає метод заміни найменшого значущого біту двійкового подання зображення LSB (Least significant bit).

Тобто LSB-стеганографія — це метод стеганографії, за якої повідомлення приховується всередині зображення, замінюючи молодший значущий біт зображення на елементи повідомлення, яке потрібно приховати.

Вважаємо, що контейнер є зображення, що може бути подане у вигляді двійкової матриці розміром $n_1 \cdot n_2 = N$:

$$Q = \begin{Vmatrix} q_{11} & \cdots & q_{1n2} \\ \cdots & \cdots & \cdots \\ q_{n11} & \cdots & q_{n1n2} \end{Vmatrix} = \begin{Vmatrix} \overline{q_1} \\ \cdots \\ \overline{q_{n1}} \end{Vmatrix}, \quad (3)$$

де q_{ij} — біти контейнера $\overline{q_j}, j = 1,2, \dots, n_1$ — вектори рядки матриці Q.

Для простоти подальшого запису рівняння перетворення контейнера трансформуємо послідовність векторів — рядків в єдиний вектор:

$$(\overline{q_1}, \dots, \overline{q_{n1}}) = (q_{11}, \dots, q_{1n2}, \dots, q_{n11}, \dots, q_{n1n2}) = (\theta_1, \dots, \theta_N) = \bar{\theta}, \quad (4)$$

де $(\theta_1, \dots, \theta_N)$ — вектор бітів контейнера після наскрізної перенумерації його бітів.

Задаємо функцію стегосистеми за допомогою наступних рівнянь:

$$\begin{cases} \theta_j = \theta_j \cdot (k_j \oplus 1) \oplus d_l \cdot k_j, \text{ де } j = \overline{1,N}, l = \overline{1,L} \\ l = \begin{cases} 1, \text{для } j = 1 \\ \sum_{i=1}^{j-1} k_i + 1, \ j \geq 2 \end{cases} \end{cases} \quad (5)$$

де θ_j — послідовність бітів контейнера стегосистеми що модифіковані згідно з інформаційним вектором D,

$\bar{k} = (k_1, k_2, \dots, k_N)$: $|\bar{k}| = L$ — двійковий вектор ключа, що має вагу Гемінга яка дорівнює L (вектор містить рівно L одиниць). Вочевидь, у визначених умовах кількість різних ключів дорівнює значенню біноміального коефіцієнта C_N^L

Зауважимо, вектор $\bar{\theta} = (\theta_1, \theta_2, \dots, \theta_N)$ згідно з рівняннями (3,4) може бути трансформований в вигляд контейнера:

$$\bar{\theta} = (\theta_1, \theta_2, \dots, \theta_N) \to \tilde{Q} = \begin{Vmatrix} \tilde{q}_{11} & \dots & \tilde{q}_{1n2} \\ \dots & \dots & \dots \\ \tilde{q}_{n11} & \dots & \tilde{q}_{n1n2} \end{Vmatrix}.$$

Рівняння (5) визначає, якщо черговий біт ключа дорівнює одиниці, то відповідний біт контейнера набуває значення чергового біту інформаційного вектору. Це означає наступне:

Твердження 1. Елементи q_{ij} та $\tilde{q}_{ij}$ контейнерів Q та $\tilde{Q}$ збігаються в одному з двох випадків:

1. Якщо в (5) біт вектора ключа дорівнює нулю, то зміна контейнера на цьому місці не відбувалася;
2. Якщо в (5) цей біт ключа дорівнює 1, а біт контейнера збігається з бітом чергового інформаційного вектора, то знову зміна контейнера не спостерігається.

Зважаючи на викладене, можливо зробити висновок, що для певних інформаційних векторів шляхом формування відповідного ключу в (5) потенційно можна забезпечити, що б вихідний та модифікований контейнери збігались: $Q = \tilde{Q}$.

Більше того, за умов певного співвідношення розміру контейнера та довжини інформаційного вектора, можливо припустити, що в контейнері можуть бути розміщені декілька повідомлень, які вибираються за допомогою відповідного ключу.

Для оцінки можливості відповіді на питання П.1 і П.2 що визначені на початку цього розділу проаналізуємо ймовірнісні характеристики модифікованого контейнера $\tilde{Q}$.

Вважаємо, що біти векторів $\bar{\theta} = (\theta_1, \dots, \theta_N)$ та $D = (d_1, \dots, d_L)$ мають біноміальний розподіл з ймовірностями відповідно:

$$P\{\theta_i = 0\} = \pi_0,\ P\{\theta_i = 1\} = \pi_1,\ \pi_0 + \pi_1 = 1,\ i = \overline{1, N}. \quad (6)$$

$$P\{d_i = 0\} = p_0,\ P\{d_i = 1\} = p_1,\ p_0 + p_1 = 1,\ i = \overline{1, L}. \quad (7)$$

Надалі, виходячи з твердження 1 оцінімо ймовірність збігу бітів пустого та модифікованого контейнерів:

$$P\{\theta_i = \tilde{\theta}_i\} = P\{k_i = 0\} + P\{k_i = 1\} \cdot P\{\theta_i = d_l\},$$

де індекс l розраховується на підставі (5).

Виходячи з (6) і (7) та враховуючи, що

$$P\{k_i = 0\} = \frac{N - L}{N}, \qquad P\{k_i = 1\} = \frac{L}{N},$$

за умов незалежності бітів пустого контейнера та інформаційного вектора для ймовірності співпадіння бітів цих контейнерів отримуємо вираз:

$$P\{\theta_i = \tilde{\theta}_l\} = \frac{N-L}{N} + \frac{L}{N} \cdot (\pi_0 \cdot p_0 + \pi_1 p_1) = 1 - \frac{L}{N}(1 - \pi_0 \cdot p_0 + \pi_1 p_1).$$

Таким чином за умов виконання зроблених припущень з останнього рівняння слідує наступне справедливість наступного твердження.

Твердження 2. В разі наближення до рівномірного розподілу бітів контейнера, або їх частини, що обрана для модифікації, має місце наступна оцінка ймовірності збігу ϑ на однакових місцях бітів пустого та модифікованого контейнерів:

$$\vartheta = P\{\theta_i = \widetilde{\theta}_i\} \approx 1 - {}^{L}/_{2N}, \text{ якщо } \pi_0 \to {}^{1}/_{2}. \quad (8)$$

Зауважимо, що оцінка (8) не залежить від розподілу бітів інформаційного вектора.

Зазначимо, що саме в випадку застосування методу LSB, внаслідок впливу процедури округлення результату під час оцифрування початкового зображення найменший значущий біт наближується до рівномірного розподілу. Це фактично обумовлює кращу застосовність цього методу для цілей стеганографії.

Для побудови статистичного критерія розрізняння контейнерів введемо функцію — індикатор події $\{\theta_i = \widetilde{\theta}_i\}$:

$$I\{\theta_i = \widetilde{\theta}_i\} = \begin{cases} 1, \text{якщо } \{\theta_i = \widetilde{\theta}_i\} \\ 0, \text{в разі } \{\theta_i \neq \widetilde{\theta}_i\} \end{cases}.$$

Введемо випадкову величину δ — міру наближення двох контейнерів:

$$\delta = \sum_{i=1}^{N} I\{\theta_i = \widetilde{\theta}_i\}. \quad (9)$$

Залежно від обраного в стегосистемі ключу $\bar{k}$ величина δ може приймати цілі значення з інтервалу $[0, N]$. Тоді ймовірність того, величина $\delta = m$ дорівнює:

$$P\{\delta = m\} = C_N^m P\{\theta_i = \widetilde{\theta}_i\}^m \cdot \left(1 - P\{\theta_i = \widetilde{\theta}_i\}\right)^{N-m}. \quad (10)$$

Нехай, $P\{\theta_i = \widetilde{\theta}_i\} = \vartheta$, тоді згідно центральної граничної теореми [20] випадкова величина δ має нормальний розподіл з математичним сподіванням $a = N\vartheta$ та дисперсією $\sigma^2 = N\vartheta(1 - \vartheta)$.

Зрозуміло, що в разі $\delta > \mathrm{C}_\alpha$ для певної заздалегідь визначеної границі критерія C_α з заданим рівнем значущості α не має підстав вважати що два контейнера за суттю є парою «пустий — модифікований» контейнери.

У випадку застосування нормального наближення для випадкової величини δ для визначення границі критерія скористуємся виразом:

$$C_\alpha = a + t_{1-\alpha} \cdot \sigma = N\vartheta + t_{1-\alpha} \cdot \sqrt{N\vartheta(1 - \vartheta)}, \quad (11)$$

де $t_{1-\alpha}$ — квантіль стандартного нормального розподілу, що відповідає рівню надійності критерія $1 - \alpha$.

Таким чином, доведено наступне твердження.

Твердження 3. Сторонній спостерігач, якій отримав два контейнера, може з рівнем значущості α визнати їх парою «пустий — модифікований» контейнери або відхилити цю гіпотезу залежно від виконання або невиконання нерівності:

$$\delta > N\vartheta + t_{1-\alpha} \cdot \sqrt{N\vartheta(1 - \vartheta)}. \quad (12)$$

Якщо спостерігач має лише один контейнер, стосовно якого він намагається визначити його статус «пустий — модифікований», то для побудови критерія розрізняння відповідних гіпотез йому потрібна інформація, що визначена в (6).

Проведене статистичне моделювання в цілому підтвердило отримані теоретичні результати, при цьому з'ясовано, що в разі достатньо великого контейнера статистичний критерій дозволяє з високим рівнем надійності виявляти модифіковані контейнери, якщо обсяг вбудованої інформації сягає величини $L \approx 0.37N$ або більше.

Таким чином, за умов невеликого обсягу інформаційного вектору відносно розміру контейнера можливо приховувати факт передавання певної конфіденційної інформації, яка стосується процедури автентифікаці в деякій корпоративній мережі.

Для цього клієнт, що має намір авторизуватись надсилає серверу модифікований за допомогою інформаційного вектору D_I контейнер $\tilde{Q}_i$ використовуючи визначену для цього напряму інформаційного обміну множину пустих контейнерів $Q_i \in \{Q_1, Q_2, \dots, Q_I\}$ ключ $\bar{k}_I$, а також сеансовий вектор ініцілізації, що використовується для зміни поточного ключа стегосистеми.

Інформаційний вектор клієнта D_I може містити дані щодо ідентифікатору пристрою з якого надсилається запит, власного ідентифікатора клієнта, часу початку сеансу взаємодії а також іншу інформацію, яка може бути ефективно використана сервером для ідентифікації клієнта.

У відповідь сервер навмання вибирає з визначеної для цього напряму інформаційного обміну множини пустий контейнер $Q_j \in \{Q_1, Q_2, \dots, Q_I\}$. Вибраний контейнер зазнає модифікації з ключе $\bar{k}_I$ та сеансовим вектором ініціалізації з використанням власного інформаційного вектору, що містить інформацію, яка необхідна клієнту для підтвердження ідентифікації сервера.

Наступним кроком клієнт в новому модифікованому контейнері надсилає серверу ґеш-образ власного паролю на підставі якого сервер завершує процедуру первинної авторизації, про що інформує клієнта наступним модифікованим контейнером. Такім чином в процедурі використовуються чотири контейнера.

Використання контейнерів — зображень додає ще одного кроку перевірки повноважень, зважаючи на те, що клієнт візуально оцінює достовірність отриманого контейнеру.

За попередніми підрахунками загальний обсяг даних, що пересилаються в процедурі не перевищує 100Кбайт, що несуттєво впливатиме швидкість її реалізації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У рамках дослідження сформульовані загальні засади побудови моделі загроз безпеки корпоративної мережі на основі концепції Zero Trust, визначені функціональні та інженерні рішення щодо побудови безконтактного апаратного засобу автентифікації клієнтів під час доступу до пристроїв системи, а також обґрунтовані ескізні рішення щодо побудови стеганографічного протоколу обміну даними в процедурах ідентифікації і управління доступом.

Пріоритетними напрямами подальших досліджень уявляється проведення розрахунків параметрів процедури обміну, проведення імітаційного моделювання та визначення практично застосовних значень параметрів протоколу, а також моделювання та вивчення поведінки протоколу в умовах кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Grechaninov, V., et al. (2022). Models and Methods for Determining Application Performance Estimates in Distributed Structures. In *Cybersecurity Providing in Information and Telecommunication Systems, 3288(1),* 134–141.

2 Grechaninov, V., et al. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. In *Cybersecurity Providing in Information and Telecommunication Systems II, 3188 (2),* 197–206.

3 Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In *Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149,* 107–117.

4 Grechaninov, V., et al. (2018). The network of situational centers of state authorities is the basis for increasing the efficiency of their activities (interaction). *Mathematical machines and systems, 3,* 32–39.
5 Skiter I., Hulak H., Grechaninov V., Klymenko V., & Ievlev N. (2021). System Approach to the Creation of Cybersecurity Centers of Critical Infrastructure. In *Cybersecurity Providing in Information and Telecommunication Systems, 3187,* 244–250.
6 Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20) (2015). *Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги* (27001:2015).
7 Гречанінов В., Оксанич І., & Лопушанський А. (2022) Використання хмарних технологій для вирішення питань інтеграції інформації у багаторівневих системах управління. *Системи керування та комп'ютери, 4,* 24–34.
8 Ferretti L., Magnanini F., Andreolini M., & Colajanni M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security, 110, 102419.*
9 Buckbee M. (2022). *What Is Zero Trust? Architecture and Security Guide*. Varonis: We Protect Data. https://www.varonis.com/blog/what-is-zero-trust
10 Dshkhunyan V., & Shan'gin V. (2004) Electronic Identification. Contactless Electronic Identifiers and Smart Cards. AST Publ., NT Press Publ.
11 Zheleznyak V., Tolubko V., Kriuchkova L., & Provozin A. (2019) Rationale for the parameters of the measuring transducer in RFID technology with inductive coupling. *Vestsi Natsyyanal'nai akademii navuk Belarusi, 64(1),* 98–109. https://doi.org/10.29235/1561-8358-2019-64-1-98-109
12 MicroID 125 kHz RFID. System Design Guide (2004). *Microchip Technology Inc.* http://ww1.microchip.com/downloads/en/devicedoc/51115f.pdf
13 MicroID 13.56 MHz RFID. System Design Guide (2004). *Microchip Technology Inc*. http://ww1.microchip.com/downloads/en/devicedoc/21299e.pdf
14 Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized (2014) (18000-1:2004).
15 Information technology — Radio frequency identification for item management — Part 2: Parameters for air interface communications below 135 kHz (2009) (18000-2:2009).
16 Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz (2010) (18000-3:2010).
17 Hulak H., Zhdanova Y., Skladannyi P., Hulak Y., & Korniiets V. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Cybersecurity: Education, Science, Technique, 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
18 Menezes A., Oorschot van P., & Vanstone S. (1997). Handbook of applied cryptography. *CRC Press.*
19 Cremers C., & Lafourcade P. (2007) Comparing State Spaces in Automatic Security Protocol Verification. *ETH Technical Report, 558.*
20 Шелест М. (1999). Цифрова стеганографія та її можливості. *Захист інформації, 1,* 11–19.
21 Стасюк О., Гнатюк С., Довгич Н., & Літош М. (2011). Сучасні стеганографічні методи захисту інформації. *Захист інформації, 1.*
22 Hulak H., et al. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Cybersecurity: Education, Science, Technique, 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
23 Sokolov, V., Skladannyi, P., & Hulak, H. (2022). Stability Verification of Self Organized Wireless Networks with Block Encryption. In *Cybersecurity Providing in Information and Telecommunication Systems, 3137,* 227–237.
24 Hulak H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. *Cybersecurity: Education, Science, Technique, 2(10),* 6–28. https://doi.org/10.28925/2663-4023.2020.10.628
25 Setiadi De R., Rustad S., Andono P., & Shidik G. (2023). Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Processing, 206.*
26 Granino A. Korn, & Theresa M. Korn (2013). Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, and Formulas for Reference and Review. *Courier Corporation.*

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

Larysa Kriuchkova
doctor of technical sciences, professor,
professor of the Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Pavlo Skladannyi
Ph.D., associate professor, head of Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Maksym Vorokhob
Lecturer of the Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

PRE-PROJECT SOLUTIONS FOR BUILDING AN AUTHORIZATION SYSTEM BASED ON THE ZERO TRUST CONCEPT

Abstract. This article describes the task of building effective solutions to increase the level of cyber security of state-level information systems in the conditions of weapons of aggression and powerful cyber attacks on critical infrastructure. A descriptive supplement to the security threat model has been developed, taking into account the concept of Zero Trust, and the threat model has been visualized, which allows you to determine the potential vulnerabilities of existing solutions regarding the construction of identification and access control subsystems. Requirements for contactless authentication hardware are defined. A functional diagram of the interaction of radio frequency identification components with passive electrical oscillating circuits has been built. A block diagram has been created algorithm of the identification system to the hardware authentication device. Defined functional and engineering solutions for the construction of contactless hardware authentication of clients during access to system devices. Grounded sketch decisions regarding the construction of a steganographic data exchange protocol in identification and access management procedures.

Keywords: cyber security; information system; cyber attack; critical infrastructure; threat model; authentication; identification; steganography; protocol; access control.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Grechaninov, V., et al. (2022). Models and Methods for Determining Application Performance Estimates in Distributed Structures. In *Cybersecurity Providing in Information and Telecommunication Systems, 3288(1),* 134–141.
2 Grechaninov, V., et al. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. In *Cybersecurity Providing in Information and Telecommunication Systems II, 3188 (2),* 197–206.
3 Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In *Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149,* 107–117.
4 Grechaninov, V., et al. (2018). The network of situational centers of state authorities is the basis for increasing the efficiency of their activities (interaction). *Mathematical machines and systems, 3,* 32–39.
5 Skiter I., Hulak H., Grechaninov V., Klymenko V., & Ievlev N. (2021). System Approach to the Creation of Cybersecurity Centers of Critical Infrastructure. In *Cybersecurity Providing in Information and Telecommunication Systems, 3187,* 244–250.

6 Technical Committee on Standardization “Information Technologies” (TC 20) (2015). *Information Technology. Methods of protecting the information security management system. Requirements* (27001:2015).
7 Hrechaninov V., Oksanych I., & Lopushanskyi A. (2022) Use of cloud technologies to solve information integration issues in multi-level management systems. *Control systems and computers, 4,* 24–34.
8 Ferretti L., Magnanini F., Andreolini M., & Colajanni M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security, 110, 102419.*
9 Buckbee M. (2022). *What Is Zero Trust? Architecture and Security Guide*. Varonis: We Protect Data. https://www.varonis.com/blog/what-is-zero-trust
10 Dshkhunyan V., & Shan’gin V. (2004) Electronic Identification. Contactless Electronic Identifiers and Smart Cards. AST Publ., NT Press Publ.
11 Zheleznyak V., Tolubko V., Kriuchkova L., & Provozin A. (2019) Rationale for the parameters of the measuring transducer in RFID technology with inductive coupling. *Vestsi Natsyyanal’nai akademii navuk Belarusi, 64(1)*, 98–109. https://doi.org/10.29235/1561-8358-2019-64-1-98-109
12 MicroID 125 kHz RFID. System Design Guide (2004). *Microchip Technology Inc.* http://ww1.microchip.com/downloads/en/devicedoc/51115f.pdf
13 MicroID 13.56 MHz RFID. System Design Guide (2004). *Microchip Technology Inc*. http://ww1.microchip.com/downloads/en/devicedoc/21299e.pdf
14 Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized (2014) (18000-1:2004).
15 Information technology — Radio frequency identification for item management — Part 2: Parameters for air interface communications below 135 kHz (2009) (18000-2:2009).
16 Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz (2010) (18000-3:2010).
17 Hulak H., Zhdanova Y., Skladannyi P., Hulak Y., & Korniiets V. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Cybersecurity: Education, Science, Technique, 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
18 Menezes A., Oorschot van P., & Vanstone S. (1997). Handbook of applied cryptography. *CRC Press.*
19 Cremers C., & Lafourcade P. (2007) Comparing State Spaces in Automatic Security Protocol Verification. *ETH Technical Report, 558.*
20 Shelest M. (1999). Digital steganography and its possibilities. *Protection of information, 1,* 11–19.
21 Stasiuk O., Hnatiuk S., Dovhych N., & Litosh M. (2011). Modern steganographic methods of information protection. *Protection of information, 1.*
22 Hulak H., et al. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Cybersecurity: Education, Science, Technique, 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
23 Sokolov, V., Skladannyi, P., & Hulak, H. (2022). Stability Verification of Self Organized Wireless Networks with Block Encryption. In *Cybersecurity Providing in Information and Telecommunication Systems, 3137,* 227–237.
24 Hulak H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. *Cybersecurity: Education, Science, Technique, 2(10),* 6–28. https://doi.org/10.28925/2663-4023.2020.10.628
25 Setiadi De R., Rustad S., Andono P., & Shidik G. (2023). Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Processing, 206.*
26 Granino A. Korn, & Theresa M. Korn (2013). Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, and Formulas for Reference and Review. *Courier Corporation.*

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.