



DOI 10.28925/2663-4023.2026.35.1371

УДК 004.056:004.89:681.5

Олейніков Іван Анатолійович

доктор філософії, старший викладач кафедри технологій цифрового розвитку,
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0001-3066-4639
i.oleinikov@duikt.edu.ua

Базака Юрій Анатолійович

старший викладач кафедри інформаційних систем та технологій,
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID: 0000-0002-4632-1649
yura.bazaka@gmail.com

Огнева Софія Євгеніївна

магістр
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0002-0835-296X
sofina.vog@gmail.com

Обушний Сергій Миколайович

кандидат економічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-6936-955X
s.obushnyi@kubg.edu.ua

**МОДЕЛЬ БЕЗПЕЧНОГО АДАПТИВНОГО КЕРУВАННЯ FDM/FFF-ДРУКОМ НА
ОСНОВІ МАШИННОГО НАВЧАННЯ В УМОВАХ КІБЕРЗАГРОЗ**

Анотація. У статті розглянуто проблему забезпечення безпечного адаптивного керування процесом FDM/FFF-друку в умовах технологічних відхилень і потенційних кіберзагроз для інформаційно-керувальної інфраструктури. Поширення адитивних технологій та інтеграція 3D-принтерів із мережевими сервісами, вбудованими обчислювальними платформами й інтелектуальними засобами моніторингу зумовлюють необхідність підвищення не лише якості виготовлення виробів, але й надійності та безпечності автоматизованого керування. Особливого значення набувають питання своєчасного виявлення технологічних аномалій, запобігання необґрунтованим керувальним втручанням, контролю достовірності вхідної інформації та обмеження несанкціонованого впливу на параметри друку. Метою дослідження є обґрунтування моделі безпечного адаптивного керування FDM/FFF-друком на основі машинного навчання, що поєднує оцінювання ризику технологічних дефектів, каскадну перевірку результатів інтелектуального аналізу та формування керувальних дій з урахуванням вимог інформаційної і функціональної безпеки. Розглянуто архітектуру інтелектуального наглядного контуру, що використовує відеодані, технологічну телеметрію та параметри завдання друку. Для ідентифікації дефектів застосовуються нейромережеві моделі класу ResNet, а для підвищення достовірності рішень – каскадна верифікація, часове згладжування оцінок ризику та механізм гістерезису. У контексті кібербезпеки розглянуто механізми розмежування прав доступу, перевірки допустимості команд G-коду, контролю цілісності конфігурацій та журналювання подій. Визначено їхню роль в обмеженні небажаних керувальних впливів і підтриманні контрольованого функціонування програмно-апаратного комплексу на базі Raspberry Pi 5. Проаналізовано наявні експериментальні результати порівняння конфігурацій інтелектуального контролю FDM/FFF-друку. Для досліджених конфігурацій наведено показники точності виявлення дефектів, частоти хибних спрацювань, затримки формування керувальних дій та частки відбракованих виробів. Порівняння демонструє можливість зменшення технологічних втрат завдяки використанню інтелектуального моніторингу й адаптивних механізмів втручання. Водночас оцінювання стійкості до цілеспрямованих кібератак визначено як окремий напрям подальших досліджень.



Ключові слова: FDM/FFF-друк; машинне навчання; адаптивне керування; кібербезпека; кіберфізична система; оцінювання ризику; ResNet; Raspberry Pi 5; безпека керувальних команд, інформаційні технології.

ВСТУП

Постановка проблеми. Розвиток адитивних технологій і поширення FDM/FFF-друку супроводжуються підвищенням вимог до якості виготовлених виробів, надійності технологічних процесів та безпечності автоматизованого керування. Процес пошарового формування виробів характеризується значною залежністю від температурних режимів, параметрів екструзії, кінематичних характеристик обладнання та властивостей матеріалу. Виникнення технологічних відхилень може спричиняти дефекти геометрії, порушення міжшарової адгезії та збільшення виробничих втрат. Традиційні засоби контролю переважно орієнтовані на підтримання встановлених параметрів і не завжди забезпечують своєчасне виявлення дефектів безпосередньо під час друку [1].

Перспективним напрямом підвищення ефективності керування є застосування машинного навчання, комп'ютерного зору та мультимодального моніторингу для автоматизованого виявлення технологічних аномалій і формування адаптивних керувальних дій [2], [3]. Водночас інтеграція 3D-принтерів із мережевими сервісами, вбудованими обчислювальними платформами та відкритими програмними інтерфейсами створює додаткові ризики несанкціонованої зміни параметрів друку, модифікації керувальних команд і порушення цілісності технологічних даних. За таких умов FDM/FFF-принтер доцільно розглядати як кіберфізичну систему, у якій інформаційні впливи можуть безпосередньо змінювати характеристики фізичного технологічного процесу.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері інтелектуального керування адитивним виробництвом зосереджені переважно на автоматизованому моніторингу, виявленні дефектів та оптимізації технологічних параметрів. У роботах [1], [2] розглянуто методи контролю FDM/FFF-друку на основі сенсорних даних і машинного навчання. Підходи до аналізу зображень сформованих шарів та реалізації зворотного зв'язку для коригування параметрів друку досліджено у працях [3], [4]. Перспективність використання глибоких нейромережових архітектур для автоматизованого виявлення та коригування технологічних відхилень продемонстровано у роботі [5], а можливості застосування моделей класу ResNet безпосередньо для виявлення дефектів 3D-друку розглянуто в дослідженні [10].

Питання кібербезпеки адитивного виробництва висвітлено у роботах [6], [7], де систематизовано загрози та продемонстровано можливі наслідки несанкціонованої модифікації цифрових моделей і технологічних даних. У дослідженні [8] розглянуто використання відеоаналізу для автентифікації процесу адитивного виробництва. Загальні принципи захисту систем операційних технологій, включаючи управління доступом, контроль цілісності та забезпечення стійкості функціонування, наведено у рекомендаціях NIST [9].

У вітчизняних дослідженнях розглянуто застосування методів машинного навчання до керування 3D-принтерами [11], використання глибоких нейронних мереж для оцінювання ризиків кіберфізичних і розподілених систем [12], [13], а також математичні підходи до оптимізації керувальних рішень [14] і моделювання загроз для систем штучного інтелекту [15].

Незважаючи на розвиток зазначених напрямів, недостатньо дослідженим залишається комплексне узгодження інтелектуального оцінювання технологічних ризиків із механізмами безпечного формування керувальних дій. Особливої актуальності набуває задача побудови адаптивної моделі, яка враховує невизначеність результатів машинного навчання, часову стійкість оцінок стану, допустимість керувальних команд та обмежені обчислювальні ресурси вбудованих платформ.

Мета статті. Метою статті є обґрунтування моделі безпечного адаптивного керування FDM/FFF-друком на основі машинного навчання, що поєднує мультимодальне оцінювання технологічного стану, каскадну верифікацію дефектів, ризикоорієнтований вибір керувальних дій та механізми забезпечення інформаційної і функціональної безпеки. Для досягнення мети розглянуто математичну формалізацію моделі, алгоритми адаптивного втручання та засоби безпечної взаємодії програмних компонентів, а також проаналізовано результати експериментальних досліджень інтелектуального комплексу керування FDM/FFF-друком на базі Raspberry Pi 5.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для розв'язання поставленої задачі використано наглядний контур FDM/FFF-друку, у якому результати комп'ютерного зору доповнюються телеметрією приводів і температурних каналів та

відомостями про поточне завдання. На відміну від автономного класифікатора зображень, така архітектура забезпечує послідовність «спостереження – оцінювання ризику – верифікація – керувальна дія – новий стан». Швидкодійні контури руху та нагрівання залишаються на рівні прошивки принтера; Raspberry Pi 5 виконує наглядові функції, що не підмінюють апаратного аварійного захисту. Стан процесу в дискретний момент часу t подано вектором:

$$s_t = (I_t, v_t, q_t), \quad (1)$$

де I_t – поточний кадр або область інтересу (ROI); v_t – вектор температур, координат, параметрів екструзії та обдуву; q_t – контекст G-коду, матеріалу й профілю друку. Попередня обробка кадру включає нормалізацію, виділення робочої області та приведення розмірності до входу мережі. Нейромережева складова базується на ознаковому поданні ResNet із наступним злиттям даних:

$$o_t = \Psi(M_\theta(C(I_t)), v_t), \quad r_t^{(0)} = R(o_t), \quad (2)$$

де C – оператор попередньої обробки, M_θ – модель виділення ознак, Ψ – оператор інтеграції з телеметрією, R – первинний оцінювач ризику; $r_t^{(0)}$ належить інтервалу $[0; 1]$.

На рисунку 1 показано структуру каскадного наглядного контуру, у якому відеоканал і телеметрія надходять до модуля оцінювання ризику, після чого формуються верифікація та керувальна дія.



Рис. 1. Структура каскадного наглядного контуру FDM/FFF-друку

Контекст G-коду враховується під час синхронізації, інтерпретації стану й вибору допустимої дії, навіть якщо безпосередній оператор злиття ознак використовує насамперед відео та телеметрію.

На першому рівні компактна модель виконує швидку індикацію підозрілих станів. Якщо оцінка ризику перевищує поріг τ_r , запускається детальніша перевірка локальних ділянок із використанням багатомасштабних ознак або сегментації; за відсутності спрацювання дорогий етап пропускається. Відповідну каскадну логіку можна подати як:

$$r_t = \begin{cases} 0, & r_t^{(0)} \leq \tau_r, \\ V(o_t), & r_t^{(0)} > \tau_r, \end{cases} \quad (3)$$

де V – уточнювальний оцінювач, r_t – верифікований ризик. Подальше прийняття рішень залежить не від окремого спрацювання, а від поведінки ризику в часі. Для придушення короточасних флуктуацій застосовується експоненціальне згладжування та лічильник послідовних підтверджень:

$$z_t = (1 - \alpha)z_{t-1} + \alpha r_t, \quad k_t = \begin{cases} k_{t-1} + 1, & r_t > \tau_v, \\ 0, & r_t \leq \tau_v, \end{cases} \quad (4)$$

де $\alpha \in (0; 1)$ визначає вагу нового спостереження; z_t – згладжена оцінка ризику; k_t – число послідовних підтверджень, τ_v – поріг верифікації. Для запобігання перемиканням режимів за коливаний поблизу порогів застосовується гістерезис; пороги упорядковано відповідно до умови $0 \leq \tau_r \leq \tau_v \leq \tau_{\text{soft}} \leq \tau_{\text{hard}} \leq 1$. Конкретні числові значення порогів визначаються профілем друку, калібруванням оцінок і вимогами до частоти хибних втручань.

Політика π враховує миттєву та згладжену оцінку, тривалість підтвердженої аномалії, поточний режим і стан друку. Розглядаються чотири рівні дій: журналювання або спостереження; попередження оператора; м'яке втручання з обмеженою корекцією швидкості, подачі, температури чи обдуву; жорстке втручання з паузою та паркуванням або зупинкою відповідно до технологічної ситуації. Вибір не зводиться до правила «дефект – негайна зупинка»: для некритичних і тимчасових відхилень пріоритетною є найменш інвазивна допустима дія.

У програмно-апаратному комплексі керувальне рішення може бути помилковим не лише через неточність нейромережі, але й через застарілі або змінені дані, порушення прав доступу чи некоректну

команду G-коду. Для цього розглянуто рольову модель ADMIN/OPERATOR/GUEST, перевірку допустимості G-коду, обмеження параметрів команд, захист з'єднань, журналювання, контроль цілісності конфігурацій і відновлення служб. Застосування таких заходів не є доказом невразливості системи до навмисних атак, але дозволяє сформулювати окрему умову допуску адаптивного впливу.

Як узгоджене подання зазначених механізмів вводиться двійкова ознака $g_t = A_t G_t H_t B_t$, де A_t характеризує авторизацію джерела команди, G_t – проходження перевірки G-коду, H_t – підтвердження цілісності та актуальності критичних даних, B_t – відповідність впливу встановленим фізичним обмеженням. Остаточна керувальна дія визначається так:

$$u_t = \begin{cases} \pi(s_t, r_t, z_t, k_t, m_t), & g_t = 1, \\ u_t^{fallback}, & g_t = 0. \end{cases} \quad (5)$$

Рівняння (5) є компактною формалізацією взаємодії політики керування з уже описаними підсистемами безпеки, а не результатом окремого експерименту з кібератаками. Резервний режим не означає автоматичну довільну зупинку в кожному випадку: за втрати довіреності команди блокується відповідне адаптивне втручання, зберігаються незалежні захисні механізми прошивки, а оператор отримує подію для підтвердження. За небезпечного фізичного стану пріоритет мають штатні механізми аварійного реагування. Для виявлення несанкціонованої зміни ваг або конфігурацій контрольні суми мають порівнюватися з еталонними значеннями, що зберігаються у захищеному контурі.

Для узагальнення розглянутих складових моделі запропоновано алгоритм безпечного адаптивного керування FDM/FFF-друком, який об'єднує в єдиному замкненому контурі отримання та перевірку мультимодальних даних, інтелектуальне оцінювання технологічного ризику, верифікацію виявлених відхилень, формування адаптивної керувальної дії та контроль допустимості її виконання. На відміну від безпосереднього передавання результату неймережевого аналізу до виконавчого контуру, запропонована послідовність передбачає багаторівневу перевірку рішення. Спочатку визначається технологічна доцільність втручання на основі поточної та згладженої оцінок ризику, результатів каскадної верифікації та стійкості аномалії в часі. Після цього сформована керувальна дія проходить окремий безпековий контур допуску, в якому враховуються авторизація джерела, допустимість G-коду, цілісність та актуальність даних і конфігурацій, а також відповідність команди встановленим фізичним обмеженням. Узагальнену блок-схему реалізації такого підходу наведено на рис. 2.

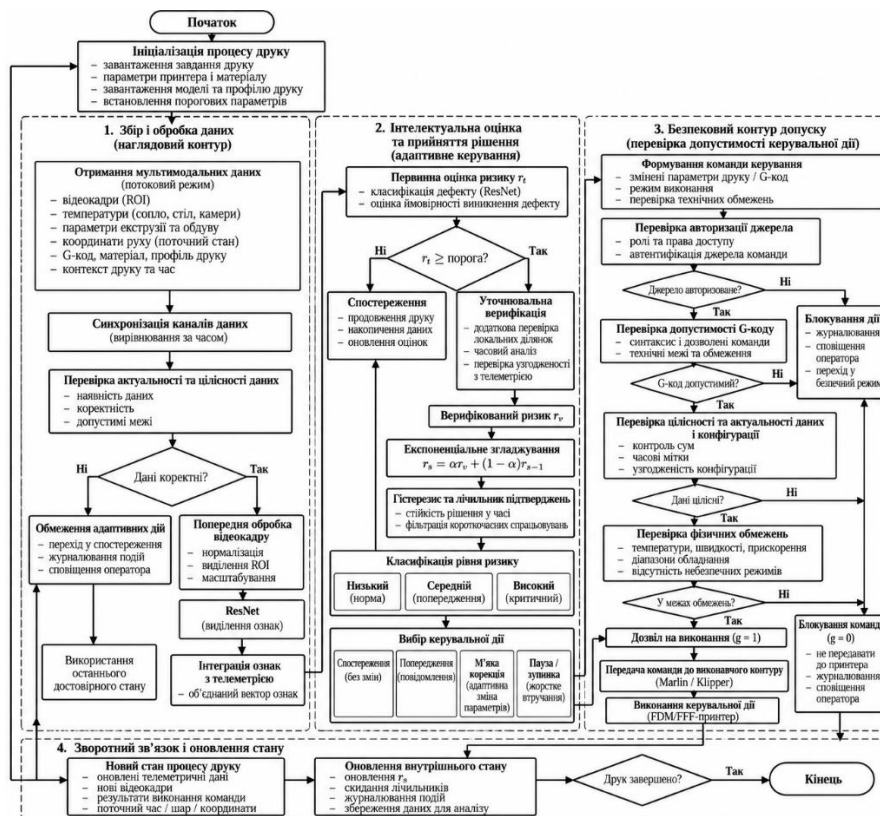


Рис. 2. Алгоритм безпечного адаптивного керування FDM/FFF-друком на основі машинного навчання



Запропонований алгоритм має циклічну структуру та реалізує замкнений наглядний контур керування. На початковому етапі виконується ініціалізація процесу друку із завантаженням завдання, параметрів обладнання, моделі та профілю друку. Після цього формується мультимодальне представлення поточного стану процесу на основі відеокadrів робочої області, температурних параметрів, характеристик екструзії та обдуву, координат руху, контексту G-коду, матеріалу і профілю друку. Отримані потоки синхронізуються за часом та перевіряються на актуальність, коректність і відповідність установленим межах. Така перевірка є принциповою, оскільки керувальне рішення не повинно формуватися на основі неповних, застарілих або потенційно спотворених даних. У разі порушення цих вимог автоматичні адаптивні дії обмежуються, подія журналюється, а система використовує останній достовірний стан або передає інформацію оператору.

Для коректних даних виконується попередня обробка відеокadру, виділення області інтересу та формування ознакового представлення засобами ResNet. Отримані ознаки інтегруються з технологічною телеметрією, після чого визначається первинна оцінка ризику $\backslash(r_t\backslash)$. Якщо її значення не перевищує встановленого порога, система продовжує спостереження без активного втручання. У разі перевищення порога активується уточнювальна верифікація, що передбачає додатковий аналіз локальних ділянок, часову перевірку та оцінювання узгодженості результатів комп'ютерного зору з телеметричними даними. Це відповідає описаній у статті каскадній логіці, за якої обчислювально складніший етап запускається лише для потенційно небезпечних станів.

Отриманий верифікований ризик не використовується для миттєвого формування керувальної команди. Для зменшення впливу короткочасних флуктуацій застосовується експоненціальне згладжування, після якого механізм гістерезису та лічильник послідовних підтверджень визначають стійкість виявленого відхилення в часі. За результатами цього етапу стан класифікується за рівнем ризику, а політика керування вибирає найменш інвазивну допустиму реакцію: продовження спостереження, попередження оператора, м'яку корекцію технологічних параметрів або жорстке втручання у вигляді паузи чи зупинки процесу. Такий підхід узгоджується із закладеним у моделі принципом, відповідно до якого виявлення дефекту не повинно автоматично спричиняти негайну зупинку друку.

Окремою особливістю запропонованого алгоритму є відокремлення рішення про необхідність керувального втручання від рішення про допустимість його фактичного виконання. Сформована адаптивною політикою команда перед надходженням до принтера проходить безпековий контур допуску. Послідовно перевіряються права та автентичність джерела команди, синтаксична і технологічна допустимість G-коду, цілісність та актуальність даних і конфігурацій, а також відповідність параметрів команди встановленим фізичним обмеженням. Лише за позитивного результату всіх перевірок формується дозвіл $\backslash(g=1\backslash)$, після чого команда може бути передана до виконавчого контуру Marlin/Klipper. За $\backslash(g=0\backslash)$ адаптивне втручання блокується, подія журналюється та передається оператору, при цьому незалежні штатні механізми захисту принтера продовжують функціонувати. Саме така логіка закладена авторами у формалізацію керувальної дії у формулі (5).

У таблиці 1 узагальнено відповідність типових загроз інформаційно-керувальному середовищу FDM/FFF-принтера, передбачених механізмів захисту та реакцій системи. Таблиця відображає функціональну логіку запропонованого узгодження, а не результати спеціальних випробувань на проникнення чи моделювання атак.

Таблиця 1

**Загрози та механізми підтримання безпечного
керування кіберфізичною системою**

Сценарій порушення	Засоби та перевірки	Допустима реакція
Несанкціонована команда	Ролі, автентифікація, журнал аудиту	Відхилення команди
Модифікація G-коду	Синтаксис, дозволені команди, технічні межі	Блокування небезпечної дії
Зміна ваг або політик	Контрольні суми та довірений еталон конфігурації	Заборона автоматичного застосування зміни
Спотворення або втрата телеметрії	Часові мітки, узгодженість каналів, контроль подій	Перевірка стану, обмеження адаптивних дій
Відмова сервісу ШІ	Моніторинг служби, watchdog, відновлення	Штатне керування та інформування оператора



На рисунку 2 показано узгодження адаптивної політики з перевітками допустимості керувальних дій. Перед передаванням команди до прошивки перевіряються права доступу, цілісність та актуальність даних, а також відповідність команди встановленим технологічним обмеженням.

Доступність контуру забезпечується розмежуванням рівнів виконання: у разі відмови сервісу інференсу система має переходити до штатного керування друком і телеметрією без необґрунтованих автоматичних корекцій. Мережевий захист, мінімізація привілеїв сервісів і журнали подій забезпечують спостережуваність інцидентів, однак достовірність каналів відео й телеметрії та стійкість до їх навмисної підміни потребують спеціальної перевірки. Таким чином, кібербезпековий аспект моделі полягає в контрольованості її інформаційних і командних інтерфейсів, а не в заявленому експериментальному виявленні кібернападів.

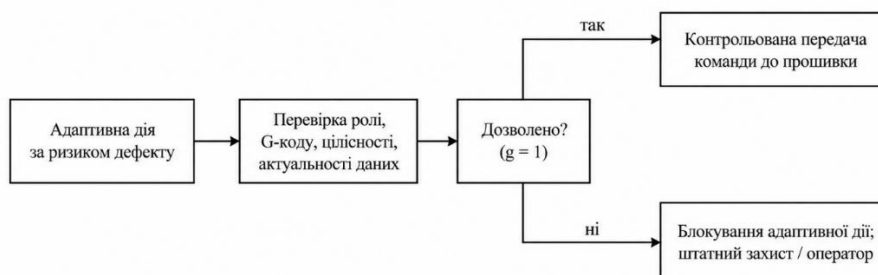


Рис. 2. Узгодження адаптивної політики з перевітками допустимості керувальної дії

Кількісне оцінювання ґрунтується на отриманих даних Test Field для п'яти конфігурацій M1–M5. Для них подано подійні частки правильного виявлення (TPR) і хибнопозитивного спрацювання (FPR), детекційні метрики mAP, затримку повного контуру «кадр – дія» та кількість хибних пауз за десять годин. Результати для досліджених конфігурацій наведено в таблиці 2.

Для інтерпретації зведених оцінок принципово важливий спосіб організації даних. У проведеному дослідженні навчальний, валідаційний, лабораторний і польовий тестові набори розділено; для Test Field передбачено неперетинання з Train і Validation за моделями виробів, профілями друку та датами реєстрації. Така побудова зменшує ризик завищення оцінок через повторне потрапляння схожих кадрів у навчання та тестування. Показники TPR і FPR у поданому порівнянні стосуються подій, тоді як mAP характеризує якість просторової детекції. Величина «хибні паузи / 10 год» відображає вже експлуатаційний наслідок роботи комплексу й не є математично тотожною FPR. Оскільки для окремих конфігурацій використано різні архітектури та способи оброблення кадрів, порівняння слід трактувати як зіставлення цілісних технічних варіантів, а не як ізольовану оцінку внеску гістерезису або однієї моделі ResNet.

Таблиця 2

Показники виявлення дефектів та експлуатаційної придатності на Test Field

Показник	M1	M2	M3	M4	M5
TPR	0,92±0,02	0,90±0,02	0,94±0,01	0,84±0,03	0,77±0,04
FPR	0,04±0,01	0,05±0,01	0,03±0,01	0,08±0,02	0,12±0,03
mAP (0,5–0,95)	0,58±0,03	0,53±0,03	0,61±0,02	0,46±0,04	–
mAP для дрібних	0,41±0,03	0,36±0,03	0,45±0,03	0,28±0,04	–
Затримка, мед., с	0,62	0,68	0,74	0,57	0,49
P95 затримки, с	0,78	0,86	0,96	0,76	0,65
Хибні паузи / 10 год	0,7	0,9	0,8	2,1	3,5

Позначення моделей: M1 – ResNet-34/FPN, режим P2, INT8, 1080p, плитки 512×512; M2 – ResNet-18/U-Net-lite, режим P1, INT8, плитки 384×384; M3 – ResNet-50/FPN, режим P3, FP16, плитки 512×512; M4 – YOLO-n, режим B2, FP16, повний кадр; M5 – ResNet-18, режим B1, INT8, повний кадр. Повні інтервали P5–P95 відповідно становлять 0,48–0,78; 0,52–0,86; 0,56–0,96; 0,44–0,76; 0,39–0,65 с. Позначення «±» відповідають вихідним оцінкам дослідження.

Найбільші TPR = 0,94, mAP = 0,61 та mAP для дрібних дефектів = 0,45 має M3; водночас вона характеризується найдовшою медіанною затримкою 0,74 с. Конфігурація M1 забезпечує TPR = 0,92 за медіанної затримки 0,62 с та найменшої зафіксованої кількості хибних пауз, що становить 0,7 на 10 год.



Отже, вибір між P2 і P3 визначається компромісом між чутливістю, затримкою та експлуатаційною ціною втручань. Наведені затримки характеризують наглядний цикл, але їх не можна ототожнювати з жорсткими часовими гарантіями приводних або температурних контурів прошивки.

Повна латентність включає час захоплення й підготовки кадру, інференсу, формування рішення, передавання команди та реакції прошивки і механіки:

$$T_{\text{frame} \rightarrow \text{action}} = T_{\text{cam}} + T_{\text{prep}} + T_{\text{infer}} + T_{\text{policy}} + T_{\text{comm}} + T_{\text{fw}} + T_{\text{mech}}. \quad (6)$$

У формулі (6) T_{cam} – час захоплення кадру, T_{prep} – час попереднього оброблення, T_{infer} – час інференсу, T_{policy} – час формування рішення, T_{comm} – час обміну з прошивкою, T_{fw} – час реакції прошивки, T_{mech} – час початку механічної реакції.

Виробничі результати порівняння режиму B0 без III, базових моделей B1-B2 та каскадних конфігурацій P1-P3 наведено в таблиці 3. Для уникнення неоднозначностей використано лише частку браку та зміну середнього часу друку за результатами порівняння конфігурацій.

Таблиця 3

Порівняльні виробничі показники конфігурацій керування FDM/FFF-друком

Режим	Модель / підхід	Брак, %	Δ часу друку, %
B0	Без III	$9,8 \pm 1,2$	0,0
B1	ResNet-18, повний кадр	$8,3 \pm 1,1$	+0,2
B2	YOLO-n, повний кадр	$7,4 \pm 1,0$	+0,4
P1	ResNet-18 + U-Net-lite	$6,2 \pm 0,9$	+0,8
P2	ResNet-34 + FPN	$5,9 \pm 0,8$	+1,1
P3	ResNet-50 + FPN, телеметрія	$5,4 \pm 0,7$	+1,6

Зменшення браку B0 від 9,8% до P2 5,9% становить 3,9 відсоткового пункта, або близько 39,8% відносно базового значення; для P3 частка браку становить 5,4%, тобто менша на 4,4 відсоткового пункта. Водночас середній час виконання завдання збільшується відповідно на 1,1% і 1,6%. На рисунку 3 наведено зміну частки браку для конфігурацій B0-P3 та інтервали відхилень, зазначені у вихідних результатах. Ці дані відображають сукупний ефект різних архітектур аналізу й керувальних політик; самостійний кількісний внесок саме засобів кіберзахисту на їх основі визначити неможливо.

Зіставлення двох груп показників засвідчує, що підвищення якості розпізнавання може супроводжуватися зменшенням частки браку за прийнятного збільшення часу друку, але не доводить причинного ефекту окремої складової каскаду без спеціального контрольного порівняння. Порогові параметри, конфігурація моделей, синхронізація телеметрії та допустимі команди потребують фіксації в журналах для відтворюваності. Механізми доступу, перевірки G-коду та контролю цілісності забезпечують архітектурні передумови безпечного виконання дій, а не підтверджену статистично стійкість до підміни даних, ін'єкцій команд чи атак на доступність.

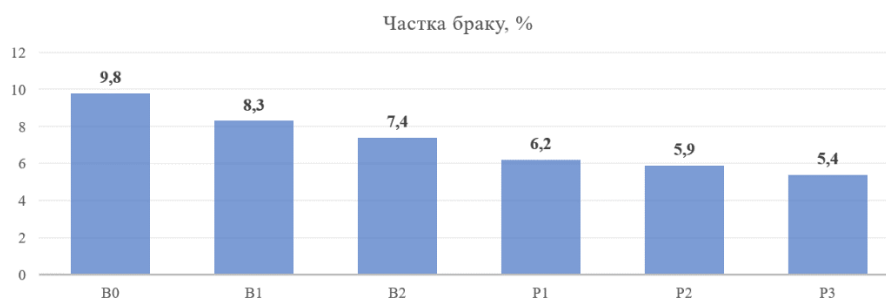


Рис. 3. Порівняння частки браку

Отже, аналіз наявних результатів підтримує доцільність каскадного ризикоорієнтованого керування FDM/FFF-друком на вбудованій платформі та включення перевірки допустимості команд до наглядного контуру. Межами отриманих висновків залишаються відсутність окремого кількісного зіставлення захищеної й незахищеної конфігурацій та відсутність спеціальних експериментів із цілеспрямованими кіберзагрозами.

**ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ**

У роботі розглянуто модель безпечного адаптивного керування FDM/FFF-друком на основі машинного навчання, що поєднує мультимодальний моніторинг технологічного процесу, каскадне виявлення та верифікацію дефектів, ризикоорієнтований вибір керувальних дій і механізми забезпечення інформаційної та функціональної безпеки.

Особливістю моделі є використання часово згладженої оцінки ризику, гістерезису та підтвердження технологічних аномалій для формування адаптивних керувальних впливів. Розглянуто узгодження політики керування з перевіркою прав доступу, допустимості команд G-коду, цілісності технологічних даних і конфігурацій програмних компонентів, що створює передумови для обмеження небажаних втручань у роботу кіберфізичної системи.

Аналіз експериментальних результатів засвідчив, що застосування досліджених інтелектуальних конфігурацій забезпечує зменшення частки браку з 9,8% у базовому режимі до 5,9% для конфігурації P2 та 5,4% для P3, що відповідає відносному зниженню на 39,8% та 44,9% відповідно. При цьому збільшення середнього часу друку становить 1,1–1,6%. Для конфігурації P2 досягнуто показника TPR 0,92 за медіанної затримки керувального контуру 0,62 с та частоти хибних пауз 0,7 на 10 годин роботи.

Отримані результати підтверджують доцільність використання каскадного ризикоорієнтованого підходу для інтелектуального керування FDM/FFF-друком на вбудованих обчислювальних платформах. Водночас кількісна ефективність механізмів протидії цілеспрямованим кібератакам потребує окремої експериментальної перевірки.

Перспективами подальших досліджень є оцінювання стійкості моделі до підміни телеметрії, модифікації G-коду та несанкціонованих керувальних впливів, а також удосконалення механізмів виявлення інформаційних аномалій і безпечного відновлення функціонування системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. He, H., Zhu, Z., Zhang, Y., Zhang, Z., Famakinwa, T., Yang, R. (2024). Machine condition monitoring for defect detection in fused deposition modelling process: A review. *The International Journal of Advanced Manufacturing Technology*, 132, 3149–3178. <https://doi.org/10.1007/s00170-024-13630-8>
2. Kozhay, K., Turarbek, S., Asselbekova, T., Ali, M. H., Shehab, E. (2024). Convolutional neural network-based defect detection technique in FDM technology. *Procedia Computer Science*, 231, 119–128. <https://doi.org/10.1016/j.procs.2023.12.183>
3. Werkle, K. T., Trage, C., Wolf, J., Möhring, H.-C. (2024). Generalizable process monitoring for FFF 3D printing with machine vision. *Production Engineering*, 18, 593–601. <https://doi.org/10.1007/s11740-023-01234-2>
4. De La Rosa, A., Armani, A., Golmohamadi, M. (2024). Defect detection and closed-loop feedback using machine learning for fused filament fabrication. *Procedia CIRP*, 126, 603–608. <https://doi.org/10.1016/j.procir.2024.08.247>
5. Brion, D. A. J., Pattinson, S. W. (2022). Generalisable 3D printing error detection and correction via multi-head neural networks. *Nature Communications*, 13, Article 4654. <https://doi.org/10.1038/s41467-022-31985-y>
6. Kumar, M., Epiphaniou, G., Maple, C. (2025). Security of cyber-physical additive manufacturing supply chain: Survey, attack taxonomy and solutions. *Computers & Security*, 157, Article 104557. <https://doi.org/10.1016/j.cose.2025.104557>
7. Alkofahi, H., Alawneh, H., Skjellum, A. (2024). MitM attacks on intellectual property and integrity of additive manufacturing systems: A security analysis. *Computers & Security*, 140, Article 103810. <https://doi.org/10.1016/j.cose.2024.103810>
8. Al Mamun, A., Liu, C., Kan, C., Tian, W. (2022). Securing cyber-physical additive manufacturing systems by in-situ process authentication using streamline video analysis. *Journal of Manufacturing Systems*, 62, 429–440. <https://doi.org/10.1016/j.jmsy.2021.12.007>
9. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., Thompson, M. (2023). Guide to operational technology (OT) security (NIST Special Publication 800-82, Revision 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r3>
10. Олейніков, І. А., Срібна, І. М. (2025). Розробка методики для пошуку дефектів 3D друку на основі моделі ResNet. Телекомунікаційні та інформаційні технології, (1), 111–119. <https://doi.org/10.31673/2412-4338.2025.014545>



11. Бондарчук, А. П., Олейніков, І. А., Бажан, Т. О. (2024). Застосування методів машинного навчання до управління 3D принтером. Телекомунікаційні та інформаційні технології, (1), 4–15. <https://doi.org/10.31673/2412-4338.2024.010415>
12. Рибальченко, Л., & Прокопович-Ткаченко, Д. (2025). Бассівський підхід у навчанні глибинних нейронних мереж для управління ризиками кіберфізичних систем. Кібербезпека: освіта, наука, техніка, 4(28), 234–245. <https://doi.org/10.28925/2663-4023.2025.28.785>
13. Палко, Д. (2025). Інтелектуальні моделі оцінки ризиків кібербезпеки в розподілених системах на основі нейромережевого підходу. Кібербезпека: освіта, наука, техніка, 3(27), 429–448. <https://doi.org/10.28925/2663-4023.2025.27.764>
14. Жданова, Ю., Шевченко, С., Спасітелєва, С., Сокульский, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 1(25), 330–343. <https://doi.org/10.28925/2663-4023.2024.25.330343>
15. Крет, Т., Марценюк, Є. (2025). Інтегрований підхід до моделювання загроз у системах штучного інтелекту. Кібербезпека: освіта, наука, техніка, 2 (30), 555–567. <https://doi.org/10.28925/2663-4023.2025.30.993>
16. Жебка, В. В., & Читулян, В. О. (2026). Модель на основі гаусівської регресії для прогнозування продуктивності корпоративних веб-систем за конфігурованих умов навантаження. Телекомунікаційні та інформаційні технології, 2(91), 215–223. <https://doi.org/10.31673/2412-4338.2026.029118>



Ivan Oleinikov

Doctor of Philosophy, Senior Lecturer, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-4051-1190
i.oleinikov@duikt.edu.ua

Yurii Bazaka

Senior Lecturer, Department of Information Systems and Technologies,
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
ORCID: 0000-0002-4632-1649
yura.bazaka@gmail.com

Sofiia Ohneva

Master's degree
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0002-0835-296X
sofiina.vog@gmail.com

Sergiy Obushnyi

PhD, Associate Professor, Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-6936-955X
s.obushnyi@kubg.edu.ua

**MODEL OF SECURE ADAPTIVE CONTROL OF FDM/FFF PRINTING BASED ON MACHINE
LEARNING UNDER CYBER THREATS**

Abstract. The article addresses the problem of ensuring secure adaptive control of the FDM/FFF printing process under technological deviations and potential cyber threats to the information and control infrastructure. The growing adoption of additive manufacturing technologies and the integration of 3D printers with network services, embedded computing platforms, and intelligent monitoring tools create a need to improve not only the quality of manufactured products but also the reliability and security of automated control. Particular attention is paid to the timely detection of technological anomalies, prevention of unjustified control interventions, verification of input data reliability, and restriction of unauthorized modifications to printing parameters. The aim of the study is to substantiate a model of secure adaptive control of FDM/FFF printing based on machine learning, which combines technological defect risk assessment, cascaded verification of intelligent analysis results, and generation of control actions considering information security and functional safety requirements. The architecture of an intelligent supervisory control loop that integrates visual data, technological telemetry, and printing task parameters is considered. ResNet-based neural network models are employed for defect identification, while cascaded verification, temporal smoothing of risk estimates, and a hysteresis mechanism are applied to improve the reliability of control decisions. In the context of cybersecurity, mechanisms for access control, G-code command validation, configuration integrity monitoring, and event logging are considered. Their role in limiting undesirable control interventions and maintaining controlled operation of a Raspberry Pi 5-based hardware and software system is identified. Existing experimental results obtained by comparing different configurations of intelligent FDM/FFF printing control systems are analyzed. The evaluated configurations are characterized by defect detection accuracy, false activation rates, control action latency, and the proportion of defective printed products. The comparison demonstrates the potential to reduce technological losses through intelligent monitoring and adaptive intervention mechanisms. At the same time, evaluating the system's resilience against targeted cyberattacks is identified as a separate direction for future research. The practical significance of the considered model lies in its potential application to the development of intelligent control systems for 3D printers with open software interfaces, particularly those based on Marlin and Klipper firmware, under limited computational resources and the need to ensure secure interaction between software components.



Keywords: FDM/FFF printing; machine learning; adaptive control; cybersecurity; cyber-physical system; risk assessment; ResNet; Raspberry Pi 5; control command security, information technologies.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. He, H., Zhu, Z., Zhang, Y., Zhang, Z., Famakinwa, T., Yang, R. (2024). Machine condition monitoring for defect detection in fused deposition modelling process: A review. *The International Journal of Advanced Manufacturing Technology*, 132, 3149–3178. <https://doi.org/10.1007/s00170-024-13630-8>
2. Kozhay, K., Turarbek, S., Asselbekova, T., Ali, H., Shehab, E. (2024). Convolutional neural network-based defect detection technique in FDM technology. *Procedia Computer Science*, 231, 119–128. <https://doi.org/10.1016/j.procs.2023.12.183>
3. Werkle, K. T., Trage, C., Wolf, J., Möhring, H.-C. (2024). Generalizable process monitoring for FFF 3D printing with machine vision. *Production Engineering*, 18, 593–601. <https://doi.org/10.1007/s11740-023-01234-2>
4. De La Rosa, A., Armani, A., Golmohamadi, M. (2024). Defect detection and closed-loop feedback using machine learning for fused filament fabrication. *Procedia CIRP*, 126, 603–608. <https://doi.org/10.1016/j.procir.2024.08.247>
5. Brion, D. A. J., & Pattinson, S. W. (2022). Generalisable 3D printing error detection and correction via multi-head neural networks. *Nature Communications*, 13, Article 4654. <https://doi.org/10.1038/s41467-022-31985-y>
6. Kumar, M., Epiphaniou, G., Maple, C. (2025). Security of cyber-physical additive manufacturing supply chain: Survey, attack taxonomy and solutions. *Computers & Security*, 157, Article 104557. <https://doi.org/10.1016/j.cose.2025.104557>
7. Alkofahi, H., Alawneh, H., Skjellum, A. (2024). MitM attacks on intellectual property and integrity of additive manufacturing systems: A security analysis. *Computers & Security*, 140, Article 103810. <https://doi.org/10.1016/j.cose.2024.103810>
8. Al Mamun, A., Liu, C., Kan, C., Tian, W. (2022). Securing cyber-physical additive manufacturing systems by in-situ process authentication using streamline video analysis. *Journal of Manufacturing Systems*, 62, 429–440. <https://doi.org/10.1016/j.jmsy.2021.12.007>
9. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., Thompson, M. (2023). Guide to operational technology (OT) security (NIST Special Publication 800-82, Revision 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r3>
10. Oleinikov, I. A., Sribna, I. M. (2025). Development of a methodology for detecting 3D printing defects based on the ResNet model. *Telecommunication and Information Technologies*, 1, 111–119. <https://doi.org/10.31673/2412-4338.2025.014545>
11. Bondarchuk, A. P., Oleinikov, I. A., Bazhan, T. O. (2024). Application of machine learning methods to 3D printer control. *Telecommunication and Information Technologies*, 1, 4–15. <https://doi.org/10.31673/2412-4338.2024.010415>
12. Rybalchenko, L., Prokopovych-Tkachenko, D. (2025). A Bayesian approach to training deep neural networks for risk management in cyber-physical systems. *Cybersecurity: Education, Science, Technique*, 4(28), 234–245. <https://doi.org/10.28925/2663-4023.2025.28.785>
13. Palko, D. (2025). Intelligent models for cybersecurity risk assessment in distributed systems based on a neural network approach. *Cybersecurity: Education, Science, Technique*, 3(27), 429–448. <https://doi.org/10.28925/2663-4023.2025.27.764>
14. Zhdanova, Yu., Shevchenko, S., Spasiteleva, S., Sokulskyi, O. (2024). Decision-making based on linear optimization in information security risk management. *Cybersecurity: Education, Science, Technique*, 1(25), 330–343. <https://doi.org/10.28925/2663-4023.2024.25.330343>
15. Kret, T., Martseniuk, Ye. (2025). An integrated approach to threat modeling in artificial intelligence systems. *Cybersecurity: Education, Science, Technique*, 2(30), 555–567. <https://doi.org/10.28925/2663-4023.2025.30.993>
16. Zhebka, V., & Chytulian, V. (2026). Gaussian Process Regression Model for Performance Prediction of Enterprise Web Systems under Configurable Workloads. *Telecommunication and Information Technologies*, 2(91), 215–223. <https://doi.org/10.31673/2412-4338.2026.029118>

Отримано редакцією журналу / Received: 09.09.26

Прорецензовано / Revised: 24.09.26

Схвалено до друку / Accepted: 26.10.26



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