© Lizunov S., Vereshchaka M, Filobok E. Analysis of computer viruses created using artificial intelligence// Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 2, pp. 256-260. ©

DOI: 10.18372/2225-5036.30.19237

АНАЛІЗ КОМП'ЮТЕРНИХ ВІРУСІВ, СТВОРЕНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Лізунов Сергій, Верещака Максим, Філобок Євгеній

Національний університет «Запорізька політехніка»

ЛІЗУНОВ Сергій Іванович, к.т.н., доцент.
Рік та місце народження: 1953 рік, м. Запоріжжя.
Освіта: Запорізький машинобудівний інститут (з 2020 року – Національний університет «Запорізька політехніка»), 1980 рік; очна аспірантура Московського енергетичного інституту, 1989 рік; Запорізький юридичний інститут МВС України, 2005 рік.
Посада: доцент кафедри інформаційної безпеки та наноелектроніки Національного університету «Запорізька політехніка».
Наукові інтереси: технічний захист інформації.
Публікації: більше 150 наукових публікацій.
E-mail: silizunov@ukr.net
Orcid ID: 0000-0001-8977-8705

ВЕРЕЩАКА Максим Павлович
Рік та місце народження: 1995 рік, м. Дунаївці, Україна
Освіта: Національний університет «Запорізька політехніка».
Посада: аспірант, Національний університет «Запорізька політехніка».
Наукові інтереси: захист інформації в інформаційних мережах, технічний захист інформації.
Публікації: більше 10 наукових публікацій.
E-mail: max111095@gmail.com.
Orcid ID: 0009-0000-7685-1774.

ФІЛОБОК Євгеній Віталійович
Рік та місце народження: 1999 рік, м. Запоріжжя, Україна.
Освіта: Національний університет «Запорізька політехніка».
Посада: аспірант, Національний університет «Запорізька політехніка».
Наукові інтереси: захист інформації в інформаційних мережах, технічний захист інформації.
Публікації: більше 10 наукових публікацій.
E-mail: filobock1999@gmail.com.
Orcid ID: 0000-0002-4105-3841.

Анотація*. Штучний інтелект (ШІ) покращує сучасний світ, відкриваючи нові можливості в різних сферах, але водночас створює нові виклики, особливо у сфері кібербезпеки. Однією із найсерйозніших загроз є використання ШІ для створення комп'ютерних вірусів, які мають здатність до самонавчання, адаптації до захисних систем і автоматичної зміни коду. Це робить їх значно складнішими для виявлення та нейтралізації порівняно з традиційними вірусами. В цій статті аналізуються різноманітні методи створення вірусів за допомогою ШІ та методи захисту від них. Першим з них є адаптивні віруси, що самонавчаються, які використовують алгоритми машинного навчання для аналізу поведінки цілей і адаптації своїх атак. Також віруси зі змінним шифруванням, що використовують штучні нейронні мережі для уникнення виявлення. Генеративно-змагальні мережі (GAN) теж активно використовуються для створення нових варіантів шкідливого коду, що ускладнює традиційні методи виявлення. Використовуються фішингові атаки на основі обробки природної мови (NLP). Ботнети з автономним управлінням на базі ШІ представляють ще одну серйозну загрозу, оскільки дозволяють здійснювати масштабні атаки без людського втручання. У відповідь на це аналізуються та впроваджуються нові методи протидії. До них відносяться антивірусні системи на базі ШІ, які можуть виявляти аномалії в поведінці програм, поведінковий аналіз, який дозволяє блокувати підозрілі програми, а також динамічний аналіз у пісочницях, що дозволяє тестувати підозрілі файли в ізольованому середовищі. Використання хмарних платформ для зберігання та аналізу даних про загрози дозволяє швидко оновлювати захисні механізми.*

Ключові слова: *штучний інтелект, комп'ютерні віруси, кіберзагрози, самонавчання вірусів, адаптивні віруси, динамічне шифрування, генеративно-змагальні мережі (GAN), фішинг, обробка природної мови (NLP), поліморфні віруси, метаморфні віруси, соціальний інжиніринг, ботнети, антивірусні системи на базі ШІ, поведінковий аналіз, пісочниці, двофакторна автентифікація, хмарна безпека.*

Постановка проблеми

Штучний інтелект (ШІ) радикально змінює сучасний світ, сприяючи розвитку технологій у багатьох галузях, таких як медицина, логістика, автомобільна індустрія і кібербезпека.

При цьому, паралельно з позитивними аспектами, ШІ може використовуватися і в злочинних цілях, особливо в кіберпросторі. Одним із тривожних наслідків використання ШІ є створення нових видів комп'ютерних вірусів. Такі віруси, написані з використанням ШІ, мають здатність до самонавчання, адаптації до захисних систем і автоматичної зміни свого коду, що робить їх складними для виявлення та нейтралізації.

Мета та постановка завдання

Актуальність роботи полягає в тому, що аналізуються загрози безпеці інформації з боку комп'ютерних вірусів, створених за допомогою штучного інтелекту, та методи захисту від них.

Швидкий розвиток ШІ відкриває нові можливості для створення і використання комп'ютерних вірусів, які мають складні властивості, таки як самонавчання, адаптація та динамічне шифрування. Ці нові типи вірусів представляють серйозну загрозу для сучасних систем кібербезпеки, ускладнюючи виявлення та нейтралізацію шкідливого коду традиційними методами.

Наразі існуючі системи захисту часто виявляються недостатньо ефективними проти таких адаптивних і самонавчальних загроз. Тому вкрай важливо розробляти нові стратегії та інструменти для боротьби з вірусами, створеними за допомогою ШІ. Дослідження новітніх методів захисту, таких як антивірусні системи на базі ШІ, поведінковий аналіз, динамічний аналіз у пісочницях та інші інноваційні підходи, є ключовими для забезпечення ефективної кіберзахисту в умовах сучасних загроз.

Виклад основного матеріалу дослідження

МЕТОДИ НАПИСАННЯ ВІРУСІВ ІЗ ВИКОРИСТАННЯМ ШІ

1. Адаптивні віруси.

Адаптивні віруси представляють собою нове покоління комп'ютерних загроз, які використовують ШІ для свого ефективного функціонування та уникнення виявлення та захисту від них. Основна особливість адаптивних вірусів полягає в їхній здатності адаптуватися до змін у системі та уникати протидійних заходів, що робить їх особливо складними для виявлення та усунення.

ШІ дозволяє їм автоматично аналізувати поведінку системи, знаходити слабкі місця та шляхи проникнення, а також модифікувати свою структуру і алгоритми з метою уникнення виявлення антивірусними програмами. Наприклад, вони можуть змінювати свою кодову базу під час розповсюдження, щоб уникнути сигнатурного виявлення, яке використовується більшістю антивірусів.

Ще однією характеристикою адаптивних вірусів є їхня здатність до самостійного навчання та еволюції. [1] Вони можуть використовувати зібрані дані про систему для покращення своїх технік нападу та захисту від виявлення. Це робить їх небезпечними не лише через їхню потужність, але й через постійне адаптування до нових умов.

2. Віруси зі змінним шифруванням.

Віруси зі змінним шифруванням (також відомі як поліморфні віруси) є особливо складними для виявлення завдяки їхній здатності змінювати власний код під час кожної інфекції. [2]

Ці віруси використовують алгоритми, які шифрують їхній основний код різними методами, що робить кожну нову версію унікальною, хоч і функціонально ідентичною.

При кожному зараженні вірус створює нову версію себе з іншим шифрувальним ключем або іншим методом шифрування, уникаючи виявлення антивірусними програмами, які шукають за сигнатурою. Однак ядро вірусу залишається незмінним, і після розшифровки виконує свою шкідливу дію.

Поліморфні віруси часто використовують ШІ для автоматизації та вдосконалення процесу шифрування, роблячи їх ще складнішими для ідентифікації. Інтелектуальні алгоритми можуть аналізувати антивірусні програми і створювати такі модифікації вірусу, які найкраще обходять захисні системи.

3. Генеративно-змагальні мережі.

Генеративно-змагальні мережі (GAN) є потужним інструментом ШІ, здатним утворювати нові дані, які за характеристиками подібні до вихідних. [3] Це стало можливим завдяки конкурентній роботі двох нейронних мереж: генератора і дискримінатора. Генератор намагається створити нові зразки, в той час як дискримінатор оцінює їх і визначає чи належать вони до реальних даних або є підробками.

У контексті комп'ютерних вірусів GAN може бути використаний для створення нових, унікальних зразків шкідливого програмного забезпечення, які здатні обходити системи виявлення вірусів. Генератор може створювати модифіковані версії вірусів, які виглядають легітимно для антивірусних програм, а дискримінатор навчається відрізняти справжні віруси від підробок, допомагаючи генератору вдосконалювати свої методи приховування.

Такі віруси можуть змінювати свою структуру або поведінку щоразу, коли вони потрапляють на новий пристрій, що значно ускладнює їх виявлення за допомогою традиційних сигнатурних методів захисту. GAN можуть також бути використані для створення поліформних або мутаційних вірусів, які постійно змінюють свій код, уникаючи детекції.

4. Фішингові атаки з використанням NLP

Фішингові атаки з використанням NLP (Natural Language Processing) набувають все більшої популярності завдяки розвитку ШІ. За допомогою NLP хакери можуть створювати дуже переконливі та персоналізовані повідомлення, які складніше відрізнити від справжніх. Ці атаки можуть використовуватися для крадіжки особистої інформації, паролів або фінансових даних.

Основні техніки фішингових атак із застосуванням NLP такі:

- аналіз мови: використання NLP дозволяє зловмисникам адаптувати мову повідомлень під стиль і тон спілкування жертви. Це робить фішингові листи або повідомлення більш правдоподібними;
- автоматизоване створення контенту: ШІ може автоматично генерувати персоналізовані повідомлення для великої кількості потенційних жертв,

враховуючи їх інтереси, поведінку в інтернеті або соціальних мережах;

- імітація діалогу: за допомогою NLP можливо створити чатботи, які імітують розмову в реальному часі, переконуючи користувача надати конфіденційні дані;
- соціальна інженерія: NLP дозволяє створювати контент, що використовує психологічні маніпуляції, апелюючи до емоцій або побоювань, тим самим підвищуючи шанси на успіх атаки.

5. Ботнети з автономним управлінням на базі ШІ.

Ботнети є однією з найпоширеніших форм кіберзагроз, де велика кількість заражених пристроїв об'єднується в єдину мережу, контрольовану зловмисниками. [4] З появою ШІ ботнети перейшли на новий рівень автономності та ефективності.

Традиційні ботнети потребували постійного контролю з боку кіберзлочинців, які надсилали команди до кожного пристрою в мережі. Однак ботнети на базі ШІ використовують автономні алгоритми, що дозволяють пристроям самостійно ухвалювати рішення та адаптувати свої дії залежно від ситуації. Це робить їх більш складними для виявлення та нейтралізації.

МЕТОДИ ПРОТИДІЇ ВІРУСАМ НА ОСНОВІ ШІ

Основні риси ботнетів з ШІ:

- адаптивне навчання: зловмисники інтегрують машинне навчання в ботнети, що дозволяє їм постійно аналізувати середовище й підлаштовувати свої атаки. Такі ботнети можуть визначати найслабкіші ланки в мережі, адаптуючи стратегії поширення;
- автономне управління: використання алгоритмів ШІ дає змогу ботнетам працювати незалежно від централізованих команд. Вони можуть координувати атаки, знаходити нові уразливості та ухилятися від засобів кіберзахисту без постійної участі людини;
- ефективне маскування: ШІ також використовується для складних методів маскування, завдяки чому ботнети важче виявити. Вони можуть змінювати свої сигнатури, використовувати шифрування та навіть імітувати звичайний інтернет-трафік, ускладнюючи їх виявлення традиційними засобами кібербезпеки;
- децентралізація: ботнети з ШІ можуть використовувати децентралізовані мережі (наприклад, peer-to-peer) для управління, зменшуючи залежність від одного командного центру, що ускладнює їх знешкодження. У разі знищення одного сегменту мережі, інші частини можуть продовжувати функціонувати автономно.

1. Антивірусні системи на базі ШІ.

Традиційні антивірусні програми використовували сигнатурний метод виявлення шкідливого програмного забезпечення (ПЗ), що полягав у порівнянні файлів із відомими зразками вірусів. Однак з появою більш складних та динамічних загроз, таких як поліморфічні та метаморфічні віруси, цей підхід стає менш ефективним.

Антивірусні системи на базі ШІ здатні виявляти нові загрози за допомогою алгоритмів машинного навчання, які аналізують поведінкові патерни програм. Завдяки глибоким нейронним мережам, ці системи можуть розпізнавати аномалії [5] та потенційно небезпечну поведінку навіть у випадку, коли конкретна загроза ще не була каталогізована. Алгоритми постійно навчаються на основі нових зразків шкідливого ПЗ, адаптуючись до нових типів атак.

Крім того, антивірусні системи на базі ШІ можуть інтегруватися з іншими інструментами кібербезпеки, створюючи багаторівневий захист від загроз. Автономні системи управління, можуть самостійно реагувати на нові загрози, застосовуючи виправлення або ізолюючи шкідливий код без втручання користувача.

2. Поведінковий аналіз.

Поведінковий аналіз — це один із найефективніших методів виявлення комп'ютерних вірусів, створених за допомогою ШІ. Цей підхід зосереджується на спостереженні за діями програмного забезпечення під час його виконання, а не на статичних характеристиках, таких як сигнатури або шифри. Застосування ШІ дозволяє аналізувати величезні обсяги даних і виявляти аномалії в поведінці програм, що може свідчити про наявність шкідливого коду.

Основні етапи поведінкового аналізу включають:

- моніторинг дій системи: антивірусні рішення в режимі реального часу стежать за усіма запусками програм і їх взаємодією з операційною системою. Це дозволяє виявити підозрілі дії, такі як несанкціонована зміна системних файлів, створення нових облікових записів або взаємодія з мережевими ресурсами;
- аналіз патернів: використовуючи алгоритми машинного навчання, антивірусні програми можуть вивчати поведінку великих обсягів даних, щоб виявити загальні патерни, притаманні шкідливому програмному забезпеченню. Це дозволяє передбачити, які дії можуть бути потенційно небезпечними;
- реакція на аномалії: у випадку виявлення підозрілої поведінки система може автоматично заблокувати або ізолювати потенційно небезпечні програми, запобігаючи їх подальшій активності та зменшуючи ризики для системи;
- адаптивне навчання: використання ШІ дозволяє системам навчатися на основі нових загроз, адаптуючи свої алгоритми виявлення до середовища загроз, що змінюється. Це робить їх більш ефективними у виявленні нових типів шкідливих програм.

Поведінковий аналіз, поєднуючи технології ШІ з традиційними методами безпеки, забезпечує більш надійний захист комп'ютерних систем. Він допомагає не лише виявляти вже відомі загрози, але й реагувати на нові атаки, що використовують інноваційні методи.

3. Динамічний аналіз у пісочницях.

Динамічний аналіз у пісочницях (sandboxing) є важливим методом виявлення і аналізу комп'ютерних вірусів, створених за допомогою ШІ. Цей метод дозволяє ізолювати підозрілі програми в контрольованому середовищі, де вони можуть виконуватись без ризику впливу на основну операційну систему та інші програми.

Основною метою динамічного аналізу є спостереження за поведінкою програми в реальному часі. [6] Під час виконання у пісочниці, віруси можуть проявляти свою активність, виконуючи шкідливі дії, такі як зміна системних файлів, крадіжка даних, чи взаємодія

з зовнішніми серверами. Аналітики мають змогу детально спостерігати за цими діями, що дозволяє виявити не лише сам вірус, а й його механізми роботи та потенційні вразливості.

Сучасні рішення для динамічного аналізу використовують алгоритми машинного навчання для виявлення аномалій, що дозволяє швидше ідентифікувати шкідливий код. За допомогою ШІ можна автоматично вивчати поведінку великих обсягів шкідливих програм, виявляючи патерни, які можуть свідчити про використання нових, раніше невідомих технік атак.

Однак, динамічний аналіз у пісочницях також має свої обмеження. Деякі складні віруси можуть розпізнавати, що вони виконуються в пісочниці, і активувати шкідливу поведінку лише в реальних умовах. Тому важливо поєднувати динамічний аналіз з іншими методами, такими як статичний аналіз, для досягнення максимальної ефективності виявлення шкідливих програм.

4. Використання шифрування та двофакторної автентифікації.

Шифрування та двофакторна автентифікація (2FA) є критично важливими методами захисту даних у боротьбі з комп'ютерними вірусами, створеними за допомогою ШІ.

Шифрування дозволяє захистити інформацію, перетворюючи її в недоступний формат для несанкціонованих користувачів. Зловмисники, які намагаються отримати доступ до даних, будуть стикаються з труднощами, оскільки шифровані дані вимагають ключа для їх відновлення. Використання потужних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), забезпечує високий рівень захисту, знижуючи ймовірність успішної атаки. У випадку витоку даних або їх підміни, шифрування забезпечує додатковий рівень безпеки, ускладнюючи доступ до чутливої інформації.

Двофакторна автентифікація є ще одним важливим елементом захисту. Цей метод вимагає двох форм підтвердження особи перед наданням доступу до облікових записів або систем. Наприклад, після введення пароля користувачеві може бути надіслано код підтвердження на мобільний телефон або електронну пошту. Це ускладнює зловмисникам доступ до акаунтів, навіть якщо вони отримали пароль. Двофакторна автентифікація суттєво підвищує безпеку, оскільки зловмиснику потрібно не тільки знати пароль, але й мати фізичний доступ до другого фактору.

Комбінування шифрування та двофакторної автентифікації створює багаторівневий захист, що значно підвищує шанси на безпечне використання інформаційних систем. У сучасному світі, де кіберзагрози стають дедалі більш складними, ці методи є невід'ємною частиною стратегії кібербезпеки.

5. Захист від соціального інжинірингу.

Соціальний інжиніринг є однією з найпоширеніших форм кібератак, що використовують людську психологію для маніпуляцій та здобуття конфіденційної інформації. Атакуючи безпосередньо на емоції та довіру користувачів, зловмисники можуть легко отримати доступ до чутливих даних, облікових записів або навіть розширити контроль над системами. Щоб захиститися від таких загроз, важливо реалізувати комплексний підхід, що включає нижчезазначені технічні та організаційні заходи.

- Навчання та підвищення обізнаності користувачів: Регулярні тренінги для співробітників і користувачів щодо методів соціального інжинірингу можуть значно знизити ризик успішних атак. Знання про те, як розпізнавати фішингові електронні листи, підозрілі дзвінки або повідомлення, допомагає створити обізнаний колектив, який здатний протистояти маніпуляціям.
- Впровадження політик безпеки: Організації повинні розробити чіткі політики безпеки, які регламентують обробку чутливої інформації, включаючи правила щодо перевірки особи при передачі даних. Використання багатофакторної автентифікації може стати ефективним захистом від несанкціонованого доступу.
- Технічні рішення: Впровадження засобів безпеки, таких як антивірусні програми та файєрволи, допомагає виявляти і блокувати шкідливі дії. Регулярні оновлення програмного забезпечення зменшують ймовірність експлуатації вразливостей, які можуть бути використані зловмисниками.
- Моніторинг активності: Організації повинні здійснювати моніторинг дій користувачів у системах для виявлення підозрілої активності. Інструменти для аналізу поведінки можуть виявляти аномалії, які вказують на можливу атаку соціального інжинірингу.
- Зворотний зв'язок та підтримка: Важливо забезпечити легкий доступ до підтримки для користувачів, які підозрюють, що стали жертвами соціального інжинірингу. Швидка реакція та зворотній зв'язок може допомогти знизити негативні наслідки атак і запобігти їх подальшому розвитку.

Захист від соціального інжинірингу вимагає постійної уваги і комплексного підходу, адже зловмисники постійно вдосконалюють свої методи. Розуміння загроз і активне протистояння їм є ключем до безпеки в інформаційній сфері.

6. Хмарні рішення з активною протидією вірусам.

Сьогодні хмарні технології стають дедалі популярнішими у сфері кібербезпеки, пропонуючи нові підходи до захисту від комп'ютерних вірусів, зокрема тих, які створені за допомогою ШІ. Хмарні рішення дозволяють забезпечити централізований контроль за загрозами та активну протидію, завдяки чому організації можуть швидко реагувати на нові виклики.

Одним з основних аспектів хмарної безпеки є використання розподілених систем для виявлення і блокування шкідливого програмного забезпечення. Ці системи аналізують великі обсяги даних у реальному часі, що дозволяє виявляти аномалії в поведінці користувачів і пристроїв. Завдяки алгоритмам машинного навчання та ШІ хмарні рішення здатні адаптуватися до нових загроз, вчитися на основі історичних даних і покращувати свою ефективність з часом.

Крім того, хмарні рішення можуть використовувати методи «активного захисту», які передбачають не лише виявлення, а й автоматичне реагування на атаки. Це може включати ізоляцію заражених систем, блокування шкідливих IP-адрес, а також автоматичне

оновлення антивірусних баз даних. Такі рішення можуть знижувати ризик поширення вірусів в організаціях, за рахунок чого зменшується час простою та збитки від атаки.

Також варто зазначити, що хмарні платформи зазвичай забезпечують можливості для резервного копіювання даних і відновлення систем після інцидентів. Це особливо важливо для організацій, які можуть стати жертвами шифрувальних вірусів, що вимагають викупу. Хмарні рішення дозволяють не лише зберігати дані в безпеці, а й швидко відновлювати їх у разі атаки.

Хмарні рішення з активною протидією вірусам забезпечують потужний інструмент для захисту від сучасних загроз, особливо у світі, де ШІ стає все більш поширеним у кіберзлочинності. Використовуючи ці технології, організації можуть не лише знижувати ризики, а й активно протистояти новим викликам у сфері безпеки.

Висновки. ШІ відкриває нові можливості для створення більш небезпечних і складних комп'ютерних вірусів. Однак паралельно з цим зростає і арсенал засобів захисту, що використовують ШІ для протидії загрозам.Боротьба з вірусами, написаними на основі ШІ, потребує розвитку інтелектуальних систем безпеки, які можуть адаптуватися до нових викликів і виявляти загрози ще до того, як вони завдають шкоди. Застосування комплексних підходів, що поєднують поведінковий аналіз, динамічний тест і хмарні технології, стане ключем до успішної боротьби з новими типами вірусів.

Список літератури

[1] Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions Електронний ресурс]. Режим доступу: https://fepbl.com/index.php/csitrj/article/view/930/1144.

[2] О.С. Саприкін. Models and methods for diagnosing Zero-Day threats in cyberspace, Вісник Сучасних Інформаційних Технологій. 4 (2021) [Електронний ресурс]. Режим доступу: https://hait.od.ua/index.php/journal/article/download/107/160/95.

[3] Generative Adversarial Nets. Advances in Neural Information Processing Systems (2014) [Електронний ресурс]. Режим доступу: https://proceedings.neurips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf.

[4] Analysis of identification of cybercrimes using cyber security analytics powered by artificial intelligence [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/383601718_ANALYSIS_OF_IDENTIFICATION_OF_CYBERCRIMES_USING_CYBER_SECURITY_ANALYTICS_POWERED_BY_ARTIFICIAL_INTELLIGENCE.

[5] Machine learning in cybersecurity: A review of threat detection and defense mechanisms [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/378208150_Machine_learning_in_cybersecurity_A_review_of_threat_detection_and_defense_mechanisms.

[6] AI Regulatory Sandboxes between the AI Act and the GDPR: the role of Data Protection as a Corporate Social Responsibility [Електронний ресурс]. Режим доступу: https: // www.researchgate.net / publication / 382496563_AI_Regulatory_Sandboxes_between_the_AI_Act_and_the_GDPR_the_role_of_Data_Protection_as_a_Corporate_Social_Responsibility.

УДК 004.67

Lizunov S., Vereshchaka M, Filobok E. Analysis of computer viruses created using artificial intelligence

Abstract. *Artificial intelligence improves the modern world by opening up new possibilities in various fields, but at the same time, it creates new challenges, especially in the realm of cybersecurity. One of the most serious threats is the use of AI to create computer viruses that have the ability to self-learn, adapt to defense systems, and automatically change their code. This makes them significantly more difficult to detect and neutralize compared to traditional viruses. Various methods of virus creation using AI are analyzed. The first is adaptive self-learning viruses that use machine learning algorithms to analyze target behavior and adapt their attacks. There are also viruses with variable encryption, which utilize artificial neural networks to avoid detection. Generative Adversarial Networks (GAN) are also actively used to create new variants of malicious code, complicating traditional detection methods. Phishing attacks based on Natural Language Processing (NLP) are employed as well. AI-based autonomous botnets present another serious threat, as they enable large-scale attacks without human intervention. In response to these threats, countermeasures are analyzed. These include AI-based antivirus systems that can detect anomalies in program behavior, behavioral analysis that allows suspicious programs to be blocked, as well as dynamic analysis in sandboxes, which enables testing of suspicious files in an isolated environment. The use of cloud platforms for storing and analyzing threat data allows for rapid updates to defense mechanisms.*

Key words: *artificial intelligence, computer viruses, cyber threats, self-learning viruses, adaptive viruses, dynamic encryption, Generative Adversarial Networks (GAN), phishing, Natural Language Processing (NLP), polymorphic viruses, metamorphic viruses, social engineering, AI-based antivirus systems, behavioral analysis, sandboxes, two-factor authentication, cloud security.*

Лізунов Сергій Іванович, к.т.н., доцент, доцент кафедри «Інформаційна безпека та наноелектроніка» Національного університету «Запорізька політехніка».

Serhii Lizunov, assistant professor of the Information Security and nanoelectronics Department, National University «Zaporizhzhia Polytechnic».

Філобок Євгеній Віталійович, аспірант Національного університету «Запорізька політехніка».

Evgenij Filobok, post-graduate student, National University «Zaporizhzhia Polytechnic».

Верещака Максим Павлович, аспірант Національного університету «Запорізька політехніка»/

Maksym Vereshchaka, post-graduate student, National University «Zaporizhzhia Polytechnic».

Отримано *29 травня 2024 року*, затверджено редколегією *26 червня 2024 року*