УДК 004.415.2
DOI https://doi.org/10.32782/2663-5941/2023.4/13

Мовчан К.О.
Український науково-дослідний інститут спеціальної техніки
та судових експертиз Служби безпеки України

РИЗИКИ КІБЕРБЕЗПЕКИ В ЕПОХУ РОБОТОТЕХНІКИ

Збільшення використання роботів у різних галузях, таких як медицина, транспорт, безпека, оборона та промисловість, на жаль, супроводжується зростаючою кількістю кібератак і загроз безпеці. Зрозуміло, що захист критичних інфраструктур від кібернетичних загроз має вирішальне значення для забезпечення безпеки і нормального функціонування суспільства.

У даній статті фокусується увага на комплексний підхід до кібербезпеки роботів, досліджуючи загрози, атаки та методи їх запобігання. Зрозуміло, що вразливі компоненти роботів включають дані, програмне забезпечення, мережі та обладнання. Для забезпечення цілісності, доступності і конфіденційності роботів рекомендується посилити шифрування, авторизацію/автентифікацію та забезпечити фізичний захист. Це допоможе уникнути перехоплення інформації, несанкціонованого доступу до роботів, а також впровадження шкідливих даних та програм.

Додатково, слід підкреслити важливість оцінки рівня кібербезпеки робототехнічних систем у різних галузях. Кожна сфера має свої особливості та унікальні загрози, тому необхідно вивчати їх з ціллю забезпечення адекватного захисту.

Зважаючи на швидкий розвиток безпілотних літальних апаратів (БПЛА), слід звернути увагу на ризики, пов'язані з їх використанням у зловмисних цілях. Кібератаки на БПЛА можуть мати серйозні наслідки, включаючи втручання у функціонування дронів та навіть можливість нанесення шкоди людям та навколишньому середовищу. Основний принцип упередження полягає у тому, щоб забезпечити надійний захист роботів від кібератак, що вимагає комплексних контрзаходів та вивчення новітніх технологій. Це включає розвиток методів шифрування, зміцнення систем авторизації та автентифікації, а також використання фізичних заходів безпеки, щоб запобігти несанкціонованому доступу до роботів.

У статті досліджуються майбутні виклики, зокрема у сферах штучного інтелекту, хмарних роботів та криміналістичного дослідження роботів. Дослідження та застосування штучного інтелекту може значно поліпшити продуктивність роботів, але також може відкрити нові ризики. Вивчення хмарних роботів допоможе зрозуміти, як хмарні технології можуть бути використані для підвищення кібербезпеки роботів. Криміналістичне дослідження роботів дозволить виявляти кібератаки та визначати їх винуватців, що є критично важливим для забезпечення кібербезпеки.

Ключові слова: *кіберзахист, роботи, операційна система роботів, криміналістичне дослідження роботів, БПЛА, кумулятивне підсумовування.*

Постановка проблеми. Останніми роками безпека комп'ютерів, пристроїв Інтернету речей, роботів і дронів стала критично важливою проблемою. В умовах, коли роботи розгортаються в життєво важливих місцях, а дрони набувають все більшого поширення, важливо розуміти їхні вразливості та потенційні загрози, щоб забезпечити безпеку як людей, так і машин.

Аналіз останніх досліджень і публікацій. Безпека роботів і дронів стала критично важливою проблемою через їхню вразливість і потенційні загрози. У випадку з роботами ризики для безпеки можуть виникнути випадково під час розробки або через непідготовлених користувачів [1, 2], тоді як проблеми кібербезпеки можуть бути спричинені зловмисниками [3], які намагаються використати важливі дані роботів і поставити під загрозу їхню цілісність, доступність і конфіденційність. Обмеження в авторизації/автентифікації [4, с. 64], шифруванні [5, с. 546] та фізичному захисті [6, с. 132] призводять до слабкої захищеності роботів і потребують модернізації. Атаки на роботів можуть призвести до різних наслідків, включаючи крадіжку інформації, глушіння бездротового зв'язку, маніпулювання поведінкою або командами [1], маніпуляції з даними [7, с. 174], фізичне пошкодження [8, с. 88] і підробку/шпигунство [5, с. 546].

Різними авторами були проведені дослідження з питань безпеки роботів. В їх роботах розглядаються атаки на безпеку, вразливості, пов'язані з ними ризики, а також надаються рекомендації

та вимоги [9] щодо захисту роботів від зловмисників. У інших дослідженнях автори звертають увагу на такі більш поширені загальні вразливості та вектори атак, як операційна система роботів (ROS – Robotic Operating System) [10, с. 192], з акцентом на перевагу вразливостей, пов'язаних з програмним забезпеченням.

Незважаючи на значну кількість наукових публікацій, присвячених проблемам захищеності роботів та дронів, стрімкий розвиток цих систем зумовлює потребу подальших досліджень цієї тематики.

Метою статті є всебічний аналіз і цілеспрямоване дослідження проблем кібербезпеки, пов'язаних з роботами і безпілотними літальними апаратами. Розглядаються вразливості, загрози і наслідки, з якими стикаються ці технології, а також досліджуються методи їх захисту. Визначаючи сфери, які потребують подальшого дослідження, що у свою чергу сприяє кращому розумінню та зменшенню ризиків кібербезпеки у сфері робототехніки та безпілотників.

Виклад основного матеріалу дослідження. Сфера робототехніки стикається з різними проблемами кібербезпеки, включаючи фізичні атаки, мережеві атаки та атаки на операційні системи (ОС). Фізичні атаки спрямовані на апаратні компоненти роботів і можуть негативно вплинути на їхню продуктивність. Наприклад, хакери можуть маніпулювати мікроконтролерами роботизованого автомобіля, що призводить до помилкових інструкцій, пошкодження компонентів або розрядки акумулятора [11, с. 211]. Мережеві атаки використовують вразливості в датчиках і комунікаційних протоколах роботів [12, с. 174]. Ці атаки можуть включати введення неправдивих даних, масштабування вимірювань або компрометацію бездротових технологій, таких як NFC і Wi-Fi. Крім того, роботи з людиноподібними рисами [13, с. 1], такі як Pepper, вразливі до таких загроз, як підробка облікових даних для входу в систему, крадіжка даних і заподіяння фізичної шкоди людям, які перебувають поблизу робота.

Що стосується безпілотників, то їхня інформаційна безпека викликає значно більше занепокоєння. Багато дронів не мають захисту та шифрування бездротового зв'язку, що робить їх вразливими до атак [14, с. 10]. Наприклад, спуфінг-атаки можуть перехоплювати і змінювати інформацію GPS, надаючи хакерам повний контроль над безпілотником. Як і звичайні комп'ютери, дрони також вразливі до зараження шкідливим програмним забезпеченням, оскільки хакери можуть впроваджувати шкідливе програмне забезпечення в системи наземних станцій через незахищені бездротові з'єднання дистанційного керування. Телеметричні дані, що використовуються для моніторингу безпілотників, часто передаються незахищеними бездротовими каналами [15, с. 115], що дозволяє перехоплювати дані, впроваджувати шкідливе програмне забезпечення та змінювати маршрути польоту. Оскільки дрони літають по заздалегідь запрограмованим та визначеним маршрутам, то маніпуляції із запрограмованими маршрутами безпілотників також несуть загрозу безпеці, оскільки це може призвести до крадіжки вантажу або доставки шкідливого вантажу. Технічні та експлуатаційні проблеми, такі як збої зв'язку, обмеження терміну служби акумуляторів і відсутність навичок пілотування, ще більше посилюють вразливість безпілотників. Природні фактори, такі як вітер, спека, дощ і туман, також можуть впливати на функціональність дронів. Крім того, дрони можуть бути перехоплені за допомогою методів глушіння Wi-Fi, що призводить до тимчасової або постійної втрати контролю над ними.

Виявлення та захист роботів від кібератак на фізичному рівні має вирішальне значення. Коли робот/дрон зазнає кібератаки, існують фізичні індикатори, які можуть допомогти ідентифікувати атаку, наприклад, зупинка робота і затримки у відповіді на навігаційні команди. Рішення для виявлення таких атак в основному реалізовані в людиноподібних роботах. Так один з підходів передбачає використання інтелектуального контроллера в поєднанні з роботом. Інтелектуальний контроллер має датчик, який вимірює параметри процесу, а логіка прийняття рішень порівнює ці вимірювання з обмеженнями. Якщо виникають будь-які порушення, активується тривога. Це рішення показало кращу ефективність у виявленні кібератак порівняно зі статистичними методами, такими як кумулятивне підсумовування (CUSUM – cumulative sum control chart) [16, с. 248].

Іншим запропонованим рішенням є інтеграція систем Intel SGX з компонентами ROS для підвищення загальної безпеки роботів [17, с. 491]. Це апаратне середовище з підтримкою безпеки, що забезпечує тестовий майданчик для роботів і гарантує безпечну обробку даних. Крім того, оновлене рішення ROS під назвою Trusted-ROS використовує апаратні обчислення для захисту незашифрованих даних, що зберігаються в пам'яті. Іншим рішенням для роботів, що використовують ROS – є використання контроллера, який обмежує поведінку робота, щоб запобігти проблемам безпеки і пом'якшити індукцію неправдивої інформа-

ції та атаки на відмову в обслуговуванні (DoS – Denial of Service).

Одним із ключових аспектів захисту роботів на мережевому рівні є раннє виявлення аномалій і вторгнень. На практиці застосовуються різні методи, серед яких найчастіше використовуються машинне навчання (ML – machine language) і статистичні методи. ML особливо ефективний у системах виявлення злочинців, які використовують розпізнавання облич. Такі алгоритми, як аналіз головних компонентів (PCA – principle component analysis) і лінійний дискримінантний аналіз (LDA – linear discriminant analysis), можна застосовувати для ідентифікації злочинців на основі даних розпізнавання обличчя. Такі фактори, як якість, освітлення та бачення, також відіграють значну роль в ефективності цих систем [18, с. 150].

У випадку застосування методу виявлення аномалій у сенсорних мережах, можна досліджувати два підходи: виявлення неправильного використання та виявлення на основі аномалій. Виявлення зловживань передбачає зіставлення сигнатур атак із сигнатурами, що контролюються, що робить його ефективним для виявлення відомих атак, але менш ефективним проти нових типів атак. З іншого боку, виявлення на основі аномалій визначає відхилення від нормальних профілів даних [19, с. 1].

Інші підходи до систем виявлення вторгнень (IDS – intrusion detection system) включають статистичні методи, непараметричні методи, підходи на основі правил, CUSUM, кластеризації даних, щільності та підходи векторної підтримки [20, с. 34].

На рівні операційних систем роботів, таких як Linux і ROS, також було виявлено численні вразливості та кібератаки. Щоб зменшити небезпеку такого типу атак, пропонуються різні рішення та інструменти для захисту ROS:

1. захист ROS на прикладному рівні, інтегрований безпосередньо в ядро ROS;

2. використання такого програмного забезпечення, як Ice та Fast-RTPS;

3. для ефективного «пом'якшення» атак на зграї БПЛА використовується ROS 2 із функціями безпеки;

4. використання віртуальних платформ, таких як RESCHU-SA, для аналізу впливу дій людини на безпеку CPS (Cyber Physical System);

5. впровадження інфраструктури безпеки та контролю доступу для запобігання ненормальному введенню даних у системи БПЛА;

6. використання методів шифрування для захисту однорангових взаємодій між вузлами ROS;

7. пропонуються різні рішення на основі шифрування, такі як CryptoROS, SROS1 і ROSRV для безпеки ROS.

Ці рішення охоплюють широкий спектр методів, від інтеграції безпеки в ядро ROS до використання шифрування для захисту зв'язку між вузлами ROS, що підвищує безпеку роботизованих систем і захисту їх від потенційних кіберзагроз.

У сфері кібербезпеки роботів існує безліч інструментів і технологій, які відіграють вирішальну роль у забезпеченні вищого рівня безпеки, особливо коли роботи взаємодіють з людьми. Одним із фундаментальних аспектів є довіра до роботів, яка може мати значні наслідки. Коли люди довіряють роботу, вони можуть мимоволі розкрити йому особисту (конфіденційну) інформацію та охоче прийняти його рекомендації. Тому встановлення надійності роботів стає першочерговим. Крім того, під час взаємодії з роботами може швидко розвиватися довіра та співпраця, особливо коли робот демонструє емоційну поведінку, яка впливає на людей і переконує їх. Розуміння впливу емоційних проявів робота на прийняття рішень людиною має вирішальне значення для формування ефективної взаємодії між людиною та роботом.

Організація безпечної роботи робота в різних сценаріях має важливе значення. Наприклад, у промислових умовах роботи повинні бути захищені від потенційних кіберфізичних атак. Зловмисники можуть використовувати вразливі місця для отримання несанкціонованого доступу, потенційно завдаючи шкоди як роботам, так і навколишньому середовищу. Надійні системи виявлення вторгнень і заходи безпеки є життєво важливими для захисту промислових роботів.

У галузі медицини ставки ще вищі, оскільки роботи часто використовуються в критично важливих програмах охорони здоров'я. Вкрай важливо переконатися, що медичні роботи стійкі до атак, оскільки вторгнення може порушити життєво важливі функції, що призведе до небезпечних для життя наслідків. Впровадження надійного шифрування, контролю доступу та регулярних оцінок безпеки є важливими кроками для забезпечення безпеки медичних роботів і пацієнтів, з якими вони взаємодіють.

Крім того, роботи, які працюють у сфері реагування на катастрофи, стикаються з унікальними проблемами. Ці роботи можуть бути чутливими до бездротових перешкод, порушуючи зв'язок і координацію під час рятувальних місій. Забезпечення

надійних протоколів зв'язку та систем резервного копіювання може підвищити стійкість роботів реагування на катастрофи проти кіберфізичних атак.

У військовому та поліцейському секторах роботи використовуються для спостереження та розвідки, і їхня безпека має першочергове значення для національної безпеки. Зловмисники можуть спробувати атакувати роботів використовуючи мережеві атаки. Але впровадження надійного шифрування та безпечних протоколів зв'язку може запобігти несанкціонованому доступу та захистити конфіденційні дані. До того ж, громадська безпека може бути під загрозою, якщо зловмисники зможуть маніпулювати роботами або дронами спостереження. Включення розширених механізмів автентифікації може захистити цих роботів, дозволяючи лише авторизованому персоналу контролювати та взаємодіяти з ними.

Сільськогосподарський сектор також покладається на роботів для виконання різноманітних завдань, і їх безпека є важливою для забезпечення безперебійної роботи. Безпілотні літальні апарати, які зазвичай використовуються в сільському господарстві, можуть бути вразливими до експлуатації через їх знаходження на відкритій місцевості. Впровадження фізичних засобів захисту та безпечних протоколів зв'язку може захистити цих роботів від несанкціонованого доступу та втручання.

Висновки. Поширення роботів у різних галузях промисловості зробило їх невід'ємною частиною нашого повсякденного життя. Однак, оскільки роботи стають все більш досконалими, пов'язані з цим ризики кібербезпеки також посилюються, що призводить до серйозних наслідків, починаючи від фінансових втрат і закінчуючи потенційною шкодою для людського життя. Ця стаття містить комплексний огляд кібербезпеки роботів, зосереджуючись на трьох найважливіших аспектах: операційні системи, мережі та фізична безпека. Аналізуючи існуючі атаки та ризики, у статті наголошується на необхідності покращення автентифікації, авторизації, шифрування та заходів фізичного захисту для пом'якшення несанкціонованого доступу, маніпулювання даними та встановлення програмного забезпечення. Аналіз показує, що машинне навчання, статистичні методи та розпізнавання образів є поширеними методами виявлення атак і розуміння їх наслідків. Виявлені наслідки атак роботів включають маніпуляції поведінкою, фізичні пошкодження, крадіжки інформації, перешкоди бездротовій мережі, підробку, шпигунство та маніпуляції даними. Крім того, дослідження заглиблюється в реальні вразливості та слабкі сторони роботів, підкреслюючи важливість захисту їх від кіберзагроз. Стаття закладає основу для майбутніх досліджень шляхом виявлення відкритих проблем, таких як інтеграція штучного інтелекту (ШІ) у робототехніку, хмарну робототехніку та криміналістичне дослідження роботів. Слід зазначити, що ШІ має величезний потенціал для підвищення продуктивності роботів, масштабованості та когнітивних можливостей. Хмарна робототехніка, як нова тенденція в IoT і хмарних обчисленнях, заслуговує на значну увагу. Крім того, враховуючи зростаючу ймовірність того, що роботи стануть мішенню хакерів, дослідження криміналістичних методів, специфічних для роботів, має вирішальне значення.

Список літератури:

1. Yaacoub, J. P., Noura, H., Salman, O., Chehab A. Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, Article 100218. 2020. https://doi.org/10.1016/j.iot.2020.100218.

2. Fosch-Villaronga E., Mahler T. Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. Computer Law & Security Review, 41, Article 105528. 2021. https://doi.org/10.1016/j.clsr.2021.105528.

3. Wang C., Tok Y. C., Poolat R., Chattopadhyay S., Elara M. R. How to secure autonomous mobile robots? An approach with fuzzing, detection and mitigation. Journal of Systems Architecture, 112, Article 101838. 2021. https://doi.org/10.1016/j.sysarc.2020.101838.

4. Jain S., Doriya R. Security issues and solutions in cloud robotics: A survey. In M. Prateek, D. Sharma, R. Tiwari, R. Sharma, K. Kumar, N. Kumar (Eds.), Next generation computing technologies on computational intelligence. Singapore: Springer Singapore. 2019. pp. 64–76.

5. Petit J., Shladover S. E. Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16, 2015, pp.546–556. https://doi.org/10.1109/TITS.2014.2342271.

6. Khalid A., Kirisci P., Khan Z. H., Ghrairi Z., Thoben K. D., Pannek J. Security framework for industrial collaborative robotic cyber-physical systems. Computers in Industry, 97, 2018, pp. 132–145. https://doi.org/10.1016/j.compind.2018.02.009

7. Sabaliauskaite G., Ng G., Ruths J., Mathur A. A comprehensive approach, and a case study, for conducting attack detection experiments in cyber–physical systems. Robotics and Autonomous Systems, 98, 2017, pp. 174–191. https://doi.org/10.1016/j.robot.2017.09.018

8. Cornelius G., Caire P., Hochgeschwender N., Olivares-Mendez M. A., Esteves-Verissimo P., Völp M., Voos H. A perspective of security for mobile service robots. In A. Ollero, A. Sanfeliu, L. Montano, N. Lau, C. Cardeira (Eds.), ROBOT 2017: Third Iberian robotics conference. pp. 88–100. Cham: Springer International Publishing. 2018.

9. Yaacoub J. P. A. Noura, H. N. Salman O., Chehab A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security. 2021. https://doi.org/10.1007/s10207-021-00545-8

10. Dieber B., Breiling B., Taurer S., Kacianka S., Rass S., Schartner P. Security for the robot operating system. Robotics and Autonomous Systems, 2017, pp. 192–203. https://doi.org/10.1016/j.robot.2017.09.017

11. Raval R., Maskus A., Saltmiras B., Dunn M., Hawrylak P. J., Hale J. Competitive learning environment for cyber-physical system security experimentation. In 2018 1st international conference on data intelligence and security (ICDIS), 2018, pp. 211–218.

12. Sabaliauskaite G., Ng G., Ruths J., Mathur, A. A comprehensive approach, and a case study, for conducting attack detection experiments in cyber–physical systems. Robotics and Autonomous Systems, 2017, pp. 174–191. https://doi.org/10.1016/j.robot.2017.09.018

13. Giaretta A., De Donno M., Dragoni N. Adding salt to pepper: A structured security assessment over a humanoid robot. In Proceedings of the 13th international conference on availability, reliability and security. 2018, pp.1–8. New York, NY, USA: Association for Computing Machinery.

14. M.F.B.A. Rahman, Smart cctvs for secure cities: Potentials and challenges, 2017. p. 35.

15. X. Lin, R. Wiren, S. Euler, A. Sadam, H.-L. Maattanen, S.D. Muruganathan, S. Gao, Y.-P.E. Wang, J. Kauppi, Z. Zou, et al., Mobile networks connected drones: field trials, simulations, and design insights, arXiv Preprint arXiv:1801.10508. 2018, pp. 115-125.

16. Sabaliauskaite G., Ng G. S., Ruths J., Mathur A. P. Empirical assessment of methods to detect cyber attacks on a robot. In 2016 IEEE 17th international symposium on high assurance systems engineering (HASE), 2016, pp. 248–251.

17. Staffa M., Mazzeo G., Sgaglione L. Hardening ros via hardware-assisted trusted execution environment. In 2018 27th IEEE international symposium on robot and human interactive communication (RO-MAN), 2018, pp. 491–494.

18. Jujjuri R., Tripathi A. K., Majji S., Prathap B. R., Patnala T. R. Detection of cyber crime based on facial pattern enhancement using machine learning and image processing techniques. In Using computational intelligence for the dark web and illicit behavior detection. 2022, pp. 150–165.

19. Mitchell R., Chen I. R. A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 46. 2014, pp.1-29 https://doi.org/10.1145/2542049.

20. Rajasegarar S., Leckie C., Palaniswami M. Anomaly detection in wireless sensor networks. IEEE Wireless Communications, 15, 2008, pp.34–40. https://doi.org/10.1109/MWC.2008.4599219.

Movchan K.O. CYBERSECURITY RISKS IN THE AGE OF ROBOTICS

The increasing use of robots in various industries, such as medicine, transport, security, defence and industry, has unfortunately been accompanied by a growing number of cyberattacks and security threats. It is clear that protecting critical infrastructures from cyber threats is crucial to ensuring the safety and normal functioning of society.

This article focuses on a comprehensive approach to robot cybersecurity, exploring threats, attacks, and methods of prevention. It is clear that vulnerable components of robots include data, software, networks, and hardware. To ensure the integrity, availability, and confidentiality of robots, it is recommended to strengthen encryption, authorisation/authentication, and physical protection. This will help to avoid interception of information, unauthorised access to robots, and the introduction of malicious data and programs.

Additionally, it is important to emphasise the importance of assessing the cybersecurity level of robotic systems in various industries. Each industry has its own characteristics and unique threats, so it is necessary to study them in order to ensure adequate protection.

Given the rapid development of unmanned aerial vehicles (UAVs), attention should be paid to the risks associated with their use for malicious purposes. Cyberattacks on UAVs can have serious consequences, including interference with the functioning of drones and even the possibility of harming people and the environment. The main principle of preemption is to ensure that robots are reliably protected from cyberattacks, which requires comprehensive countermeasures and the study of the latest technologies. This includes developing encryption methods, strengthening authorisation and authentication systems, and using physical security measures to prevent unauthorised access to robots.

The article explores future challenges, in particular in the areas of artificial intelligence, cloud robots and forensic robotics. The research and application of artificial intelligence can significantly improve the performance of robots, but it can also open up new risks. The study of cloud robots will help to understand how cloud technologies can be used to improve the cybersecurity of robots. Forensic robotics research will help detect cyberattacks and identify their perpetrators, which is critical to ensuring cybersecurity.

Key words: *cybersecurity, robots, robot operating system, forensic investigation of robots, UAVs, cumulative summation.*