МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

МАТЕРІАЛИ

XII Всеукраїнської науково-технічної конференції з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2024

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю [Електронний ресурс]. – Миколаїв : НУК, 2024. – 234 с.

У збірнику подано матеріали XII Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

УДК 004.056.5;057.2

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО КАТЕГОРИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Автор: *Злочевська О.В., магістрантка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Критична інфраструктура (КІ) будь-якої країни характеризується покладеними на неї особливими функціями, що є життєво важливими для населення та держави. При цьому порушення у виконанні цих функцій певним об'єктом критичної інфраструктури (ОКІ) з належними показниками якості може мати негативний вплив не тільки в межах однієї країни, а й зачіпати інтереси інших країн, КІ котрих є взаємопов'язаними фізично або за економічними і політичними договорами [1, 2]. Наявні в сучасному світі тенденції до зростання організованої злочинності і до посилення екстремізму та тероризму знаходять своє віддзеркалення в кіберпросторі. При цьому типово злочинні технології, зокрема хакерські атаки, використовуються за підтримки урядів як для проведення інформаційних так і для проведення звичайних військових і терористичних операцій. Тому забезпечення безпеки КІ є складовою задачі забезпечення національної безпеки особливо в Україні, в умовах військового стану.

Розв'язок проблеми захисту КІ вимагає комплексного вирішення питань нормативно-правового, організаційного, технологічного і технічного забезпечення з врахуванням ступеня критичності кожного ОКІ і кожного об'єкта критичної інформаційної інфраструктури (ОКІІ). Цій проблемі присвячені роботи багатьох науковців [3-9], однак забезпечення кіберготовності і кіберстійкості КІ вимагає в умовах динамічного кіберпростору багатократного аналізу стану інформаційної безпеки (ІБ) на ОКІ і швидкого прийняття адекватних рішень, шо неможливо без впровадження засобів автоматизації.

Метою даної роботи є розробка структури системи підтримки прийняття рішень щодо категоризації об'єктів критичної інфраструктури.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– провести аналіз відкритих літературних джерел і визначити типові процедури категоризації ОКІ, їх алгоритми, вхідні та вихідні дані системи підтримки прийняття рішень (СППР) щодо категоризації ОКІ;

– розробити структуру СППР щодо категоризації ОКІ.

Нормативно-правову базу категоризації ОКІ в загальному випадку складають:

– Директиви Європейського Союзу [1, 2];

– Закони України: «Про критичну інфраструктуру» [10], «Про основні засади забезпечення кібербезпеки України»;

– Стратегія кібербезпеки України та План реалізації Стратегії кібербезпеки України;

– Постанови Кабінету міністрів України: №518 (2019 рік), № 943 (2020 рік), №1109 (2020 рік), №821 (2022 рік);

– Наказ № 23 Адміністрації ДССЗЗІ (2021 рік).

При цьому протягом 2020-2024 років ці документи неодноразово коригувалися. Для конкретного сектору і підсектору можуть бути наявні додаткові документи у вигляді нормативних документів (наприклад, «Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг», затверджене Постановою № 4 Правління Національного банку України від 16.01.2021) або рекомендацій (наприклад, Recommendation on Cyber Resilience, розроблені Міжнародною асоціацією класифікаційних товариств для морської галузі).

Методичну основу категоризації ОКІ складають:

– Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави, затверджений Постановою КМУ №1109;

– Порядок віднесення об'єктів до об'єктів критичної інфраструктури затверджений Постановою КМУ №1109;

– Порядок формування переліку об'єктів критичної інфраструктури, затверджений Постановою КМУ № 943;

– Порядоквнесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної

інфраструктури, його формування та забезпечення функціонування, затверджений Постановою КМУ № 943;

– Методика категоризації об'єктів критичної інфраструктури, затверджена Постановою КМУ №1109 [11];

– Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури, затверджені Наказом № 23 Адміністрації ДССЗЗІ [12];

– Порядок здійснення моніторингу оцінки рівня безпеки об'єктів критичної інфраструктури, затверджена Постановою КМУ №821.

Аналіз нормативних документів дозволив виявити наступні типові процедури категоризації ОКІ:

– створення державою списку основних послуг, надання яких визначає належність досліджуваного об'єкта до ОКІ, із визначеними секторами і під секторами і відповідальними органами;

– створення робочої групи в межах сектору або під сектору;

– ідентифікація ОКІ у відповідному секторі або під секторі КІ;

– проведення категоризації ОКІ;

– проведення категоризації ОКІІ;

– створення секторального переліку ОКІ;

– подання відомостей щодо категорованих ОКІ галузі до Національного переліку ОКІ і формування державного реєстру ОКІ;

– моніторинг оцінки рівня безпеки ОКІ.

Наведені типові процедури представлені у порядку їх виконання, і кожна з них здійснюється за окремим алгоритмом. Зокрема, віднесення ОКІ до певної категорії критичності [11, 12] здійснюється шляхом визначення інтервалу, в який потраплє нормована оцінка критичності $РК_{ОКІ}$ даного ОКІ, отримана за секторальними і міжсекторальними критеріями оцінювання. Віднесення об'єкта інформаційної інфраструктури до ОКІІ даного ОКІ – на підставі висновку про суттєвий вплив об'єкта інформаційної інфраструктури на процес виконання ОКІ його основних функцій, що отримується шляхом перевірки ряду умов. Узагальнений алгоритм категоризації та відповідна інформаційна модель наведені в [9] і охоплюють процедури оцінювання за секторальними і міжсекторальними критеріями.

Прийняття рішень стососовно категоризації ОКІ здійснюється за ієрархічною схемою. На міжнародному рівні приймаються рішення щодо

визначень критичних інфраструктур, принципів їх захисту і взаємодії держав у цій галузі. На основі міжнародних нормативних документів і міжнародних договорів на рівні держави:

– приймаються рішення щодо основних функцій ОКІ, секторів і підсекторів критичної інфраструктури держави, порядку формування національних реєстрів;

– визначаються відповідальні за процедури категоризації та ведення реєстрів особи і структурні підрозділи на рівні держави та правила формування відповідальних структурних підрозділів і осіб на рівні секторів (робочих груп);

– визначається формат і порядок документообігу з категоризації;

– визначаються критерії оцінювання критичності, рівні критичності і умови віднесення до них ОКІ та ОКІІ;

– розробляються та оприлюднюються методики оцінювання рівнів критичності.

На рівні секторів приймаються рішення щодо:

– створення робочих груп;

– ведення секторальних переліків ОКІ та ОКІІ;

– передавання даних до національних реєстрів;

– порядку моніторингу оцінки рівня безпеки ОКІ;

– розробляються пропозиції щодо змін да доповнень переліків основних функцій ОКІ, секторів і підсекторів критичної інфраструктури держави.

На рівні робочої групи приймаються рішення щодо:

– категоризації ОКІ;

– категоризації ОКІІ;

– оцінкювання рівня безпеки ОКІ та його динаміки за результатами моніторингу;

– необхідності удосконалення систем захисту ОКІ.

На рівні ОКІ приймаються рішення щодо:

– застосування певних методів і засобів захисту ОКІ та моніторингу його рівня безпеки;

– визначення можливих наслідків порушень виконання основних функцій ОКІ;

– визначення можливих наслідків порушень функціонування об'єктів інформаційної інфраструктури ОКІ;

– визначення ступеня впливу об'єктів інформаційної інфраструктури ОКІ на виконання ОКІ його основних функцій.

На міжнародному рівні, рівні держави і секторів приймаються організаційні рішення, а на рівні ОКІ – рішення щодо організаційного і технічного захисту ОКІ, рішення щодо взаємного впливу структурних складових ОКІ, рішення щодо наслідків порушення штатного функціонування структурних складових ОКІ та ОКІ в цілому. Рішення, прийняті на цих рівнях є вхідними даними для прийняття рішень ра рівні робочої групи. На кожному рівні до СППР повинні мати доступ користувачі із різними правами.

Структура СППР має містити:

1) блок інтерфейсу із розмежуванням прав доступу;
2) блок даних, які поділяються на:

– вбудовані дані, визначені на рівні держави;

– відносно статичні дані, визначені на рівні секторів і підсекторів, які стосуються робочих груп, секторальних переліків ОКІ та ОКІІ, а також містять відомості, які необхідні для заповнення звітної документації на рівні робочої групи, під секторів і секторів;

– динамічні дані, визначені на рівні ОКІ;

3) блок оцінювання критичності;
4) блок формування звітності.

Висновки

В даній роботі проведено аналіз відкритих літературних джерел і визначені типові процедури категоризації ОКІ, їх алгоритми, вхідні та вихідні дані СППР щодо категоризації ОКІ, розроблена структура СППР.

Список літератури:

1. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 06 липня 2019 року "Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу". URL: https://zakon.rada.gov.ua /rada/show/984_013-16#n3

2. Директива Ради 2008/114/ЄС від 08 грудня 2008 року "Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту". URL: https://zakon.rada.gov.ua/ rada/ show/984_002-08#n4

3. Limba, Tadas, et al. Cyber security management model for critical infrastructure. (2019). *The International Journal Entrepreneurship and Sustainability*. Issues ISSN 2345-0282 (online) URL: http://jssidoi.org/jesi/ 2017 Volume 4 Number 4 (June) http://doi.org/10.9770/jesi.2017.4.4(12)

4. Osei-Kyei, Robert, et al. Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reductio*. V.60 (2021): 102316. URL: https://www.sciencedirect.com/science/article/abs/pii/S221242092100282X

5. Бірюков Д. С. Захист КІ в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки*. 2015. № 3-4. С. 155-170. – URL: http://nbuv.gov.ua /UJRN/nivanb_2015_3-4_14.

6. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/ p_303_79299367.pdf

7. Зелена книга з питань захисту КІ в Україні (друга версія проекту документа). URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf

8. Рогов П.Д., Ворович Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері. *Зб. наук. праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського*. 2017. № 1. С. 64-72. URL: http://znp-cvsd.nuou.org.ua/article/view/125525

9. Турти М.В., Злочевська О.В. Інформаційна модель категоризації об'єктів критичної інфраструктури. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2022. С.140-147. URL: https://www.nuos.edu.ua/wp-content/uploads/2023/05/ SPIBT-2022-Materiali-s-obkladinkoju.pdf

10.Закон України "Про критичну інфраструктуру". URL: https://zakon.rada.gov.ua/ laws/show/1882-20#Text

11.Методика категоризації об'єктів КІ, затверджена Постановою Кабінету міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 р. №1109. URL: https://zakon.rada.gov.ua/ rada/show/1109-2020-%D0%BF#Text

12.Наказ № 23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». URL: https://zakon.rada.gov.ua/ rada/show/v0023519-21#Text

УДК 004.056.53

АНАЛІЗ СИСТЕМИ ЗАХИСТУ ПЛАТФОРМИ BLYNK

***Автор**: Зобова Е.В., студентка, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна*

***Науковий керівник:** Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ.

Інтернет речей (IoT) — це інформаційна мережа фізичних об'єктів (датчиків, машин, автомобілів, будівель та інших предметів), яка об'єднує всі ці об'єкти та дозволяє їм взаємодіяти один з одним для досягнення спільних цілей.

У наш час, коли світ стрімко рухається до цифрової трансформації, Інтернет речей стає невід'ємною частиною нашого життя. Мільярди пристроїв, від смартфонів до промислових датчиків, підключені до мережі, створюючи безмежні можливості для автоматизації та аналізу даних. Однак, разом із зростанням кількості підключених пристроїв, зростають і ризики. Кіберзагрози, такі як хакерські атаки, віруси та шкідливе програмне забезпечення, стають все більш витонченими та спрямованими на вразливості IoT-систем. Захист цих систем набуває критичного значення, оскільки від цього залежить безпека не тільки окремих користувачів, але й цілих інфраструктур.

Метою роботи є дослідити вбудовані системи захисту для середовища розробки Інтернет речей – Blynk.

Основна частина.

Blynk – це повний набір програмного забезпечення, необхідного для прототипування, розгортання та віддаленого керування підключеними електронними пристроями будь-якого масштабу: від персональних IoT проектів до мільйонів комерційних підключених продуктів.

Користувачами системи, є як новачки в розробці електронних пристроїв так і професійні розробники. Розробник Blynk – це спеціальний

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

XII Всеукраїнська науково-технічна конференція
з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич