Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

X ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

13-14 грудня 2022 р.

Миколаїв ■ НУК ■ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2022

МАТЕРІАЛИ

X Всеукраїнської науково-технічної конференції з міжнародною участю

13–14 грудня 2022 року

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

МИКОЛАЇВ • НУК • 2022

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 X Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2022. – 209 с.

У збірнику подано матеріали X 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

МОДЕЛЬ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ОРГАНІЗАЦІЇ

Автори: *Божаткін С.М., ст. викладач; Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Будь-яка організація намагається знизити залишкові ризики інформаційної безпеки (ІБ) [1] за допомого економічно доцільних систем захисту інформації (СЗІ) [2, 3].

З точки зору системного аналізу СЗІ є підсистемою організації і має власну мету – запобігання загрозам її ІБ, яка підпорядкована цілям організації як системи в цілому. СЗІ впливає на виробничу діяльність всіх підрозділів організації, забезпечуючи цілісність і доступність інформації, яка необхідна для функціонування організації, та забезпечуючи конфіденційність інформації, яка захищається згідно загальнодержавних вимог або на вимогу власника. Відповідно, існують прямі непрямі зв'язки СЗІ з іншими підрозділами організації і з зовнішнім середовищем, які впливають на ефективність СЗІ і показники якості функціонування організації і можуть бути представлені у вигляді моделей різного типу [4].

Метою даної роботи є побудова узагальненої суб'єктно-об'єктної мотиваційної моделі процесів інформаційної безпеки організації.

Для досягнення поставленої мети необхідно визначити типи процесів ІБ організації, об'єкти і суб'єкти цих процесів та мотивацію їх поведінки.

Серед процесів ІБ організації можна виокремити ряд наступних стандартних процедур:

- віднесення інформації до категорії інформації з обмеженим доступом (ІзОД);
- виявлення загроз безпеці активів організації;
- створення механізмів оперативного реагування на загрози, відшкодування та локалізації збитків, послаблення негативного впливу наслідків порушень ІБ на стратегічні цілі організації;
- розслідування інцидентів ІБ;
- прогнозування подій ІБ з метою попередження інцидентів;

– планування модернізації і впровадження засобів управління ризиками ІБ;
– впровадження засобів управління ризиками;
– контроль ефективності СЗІ, виявлення і усування недоліків.

В розроблюваній моделі в якості об'єктів розглядаються:
– активи, що мають для організації певну цінність та власні множини вразливостей;
– цінність активу, яка може бути виражена в монетарній бальній чи якісній формі і може бути повністю або частково втрачена внаслідок успішної експлуатації загрозами певних вразливостей;
– вразливості інформаційно-комунікаційної системи (ІКС) та вразливості СЗІ, що впливають на ймовірність реалізації загрози;
– збитки або втрати, спричинені негативними наслідками реалізації загрози для бізнесу і витратами на відновлення активу і СЗІ;
– ризик – ймовірний збиток організації в разі реалізації загрози ІБ.

Суб'єктами в розроблюваній моделі є:
– власник активів, який створює СЗІ з метою їх захисту;
– джерела загроз, зокрема, зловмисник, що створює цілеспрямовані загрози, а також природні події, технічні відмови, помилки персоналу, фізичні пошкодження, що мають випадковий характер;
– загрози ІБ, які ініціюють процес експлуатації вразливостей;
– СЗІ, яка протидіє загрозам.

Кожен суб'єкт моделі може застосовувати різні стратегії для досягнення власних цілей.

Метою власника є отримання максимального прибутку, для чого необхідно зберігати ресурси і репутацію організації, та зменшувати поточні витрати і потенційні втрати. Тому дії власника мотивуються його бажанням зберегти активи, знизити ризики і не витрачати надмірні кошти на СЗІ, тобто власник в своїх діях керується принципом «розумної достатності». Власник визначає інформаційні ресурси, що містять ІзОД, цінність активів, критерії прийняття ризиків; ініціює створення СЗІ і приймає участь у процесах створення механізмів оперативного реагування на загрози, відшкодування та локалізації збитків, послаблення негативного впливу наслідків порушень ІБ, плануванні модернізації і впровадження засобів управління ризиками.

Діяльність зловмисника може бути мотивована бажанням помсти, бажанням отримати конкурентні переваги чи реалізувати певну шахрайську схему тощо. В будь-якому разі зловмисник зацікавлений в організації несанкціонованого використання активів шляхом створення загроз, що збільшують ризики в ІКС організації і прямим чи непрямим чином впливають на бізнес-процеси.

Кожна загроза намагається успішно реалізуватися за рахунок експлуатації вразливостей, асоційованих з активами, і наявних недоліків СЗІ, тобто вразливостей СЗІ.

Головною метою діяльності СЗІ є зниження або утримування ризиків на прийнятному для організації рівні, для чого необхідно виявляти і усувати вразливості, вчасно виявляти загрози і зменшувати їх негативний вплив. Відповідно СЗІ приймає участь у всіх процесах ІБ організації після свого створення, що є окремою процедурою.

Суб'єкти моделі, що є стохастичними процесами не мають мотивації для здійснення цілеспрямованого негативного впливу, однак вони здатні ініціювати техногенні, антропогенні і природні загрози і створювати ризики ІБ в ІКС.

На рис.1 наведена розроблена узагальнена суб'єктно-об'єктна мотиваційна модель процесів ІБ організації, яка побудована на основі стандарта ISO/IEC 27005:2011 [5]. На рис.1 суб'єкти позначені овалами, об'єкти – прямокутниками, причинно-наслідкові зв'язки – суцільними лініями, а цільові відношення суб'єктів системи – пунктирними лініями.

Наведена на рис.1 модель відображає сукупність об'єктивних і суб'єктивних зовнішніх і внутрішніх факторів, які впливають на стан інформаційної безпеки, що характеризується ризиком, зумовленим однією загрозою, яка в загальному випадку формується в результаті цілеспрямованих дій зловмисника і впливу випадкових факторів різної природи. Для множини загроз повинен розглядатися сумарний ризик, спричинений множиною загроз, асоційованою з активом.

Отримана модель є семантичною мережею, в якій використовуються такі типи зв'язків як «має», «прагне», «створює», «знизити», «збільшити», «зберегти», «використовує».

Висновки. В даній роботі визначено типів процесів ІБ організації, об'єкти і суб'єкти цих процесів та мотивацію їх поведінки.

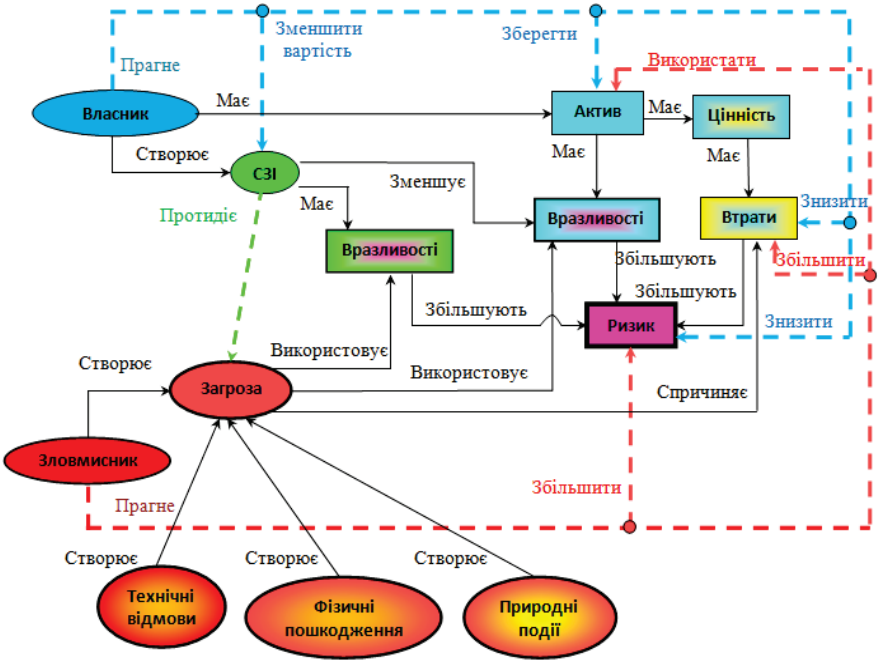

Рисунок 1 – Узагальнена модель процесів інформаційної безпеки організації

Список літератури:

1. Arnold R. Cybersecurity: A Business Solution: An executive perspective on managing cyber risk. Winston-Salem: Threat Sketch, LLC, 2017. – 100 с. [URL]: https://books.google.com.ua/books?id=zu44DwAAQBAJ&pg =PA22&redir_esc=y#v=onepage&q&f=false

2. Архипов О.Є., Архипова Є.О. Ризиковий підхід до визначення обсягу оптимальних інвестицій у безпеку інформації / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность. Материалы XV Международной научно-практической конференции ИТБ-2015. (21 жовтня 2015 р., м. Київ). – К.: ИПРИ НАН Украины, 2015. –

250 с. – С.12-17. [URL]: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-15_AA_risk2_konf.pdf

3. Корченко О.Г., Гнатюк С.О, Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально.-наукових. та науково-практичних видань НА СБ України, 2014. – 190 с.

4. Турти М.В, Книжник Р.О. Методика визначення оптимальності інформаційних моделей в галузі інформаційної безпеки //Матеріали III Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».- Миколаїв: НУК, 2013. – С.148-153.

5. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. [URL]: https://www.iso.org/standard/ 56742.html

УДК 004.056.5; 057.2

ІНФОРМАЦІЙНА МОДЕЛЬ ОЦІНЮВАННЯ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Автор: *Гайванюк І.О., магістр, 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*

Сучасний кіберпростір є середовищем, яке дозволяє здійснювати електронні комунікації у фаховій діяльності людини або в процесі реалізації суспільних відносин. Безпека кіберпростору держави повинна забезпечуватися так саме, як безпека її території на суші, в повітрі і морі. Кіберпростір утворюється в результаті функціонування сумісних комунікаційних систем з використанням глобальних і локальних мереж передачі даних.

Для захисту інформації застосовуються комплексні системи захисту інформації (КСЗІ), необхідність застосування, порядок впровадження і оцінювання ефективності котрих регламентується низкою законів України, міжнародними нормативними документами, норма-

ЗМІСТ

Секція 1. Інформаційна безпека транспортних засобів і систем 3

Особливості управління проєктами інформаційної безпеки об'єктів морської критичної інфраструктури *Блінцов В.С., Буруніна Ж.Ю.* 3

Особливості формування концепції інформаційної безпеки для ініціативи «Флот морських дронів України» *Нужний С.М.* 7

Секція 2. Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах 16

Дослідження адаптивної системи активного захисту мовної інформації у виділеному приміщенні *Демідов І.А.* 16

Комбіновані методи забезпечення інформаційної безпеки *Кобзєв В.Г.* 20

Розробка КСЗІ для об'єкту критичної інфраструктури воднотранспортного комплексу *Крюк А.С.* 23

Ідентифікація стану пристроїв IoT для задач захисту інформації *Лисинчук В.В.* 29

Розробка блоку кіберзахисту для КСЗІ на об'єкті критичної інфраструктури воднотранспортного комплексу *Майгур О.І.* 34

Аналіз методик оцінювання ефективності звукоізоляції в захисті мовної інформації *Сизов М.О.* 40

Аналіз захищеності бездротових точок доступу в мережі WI-FI *Соболєв В.В.* 45

Робота та моніторинг комп'ютерних мереж в умовах воєнного стану *Трибулькевич С.Л.*; *Трибулькевич В.В.* 48

Розробка комплексної системи захисту інформації режимно-секретного відділу морського порту *Харченко М.С.* 56

Секція 3. Правові аспекти діяльності в галузі інформаційної безпеки....61

Правові аспекти діяльності в галузі інформаційної безпеки *Матраєва Д.В.* 61

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації ***67***

Аналіз процесу ідентифікації ризиків інформаційної безпеки *Баронова О.А.*; *Божаткін С.М.*; *Турти М.В.* 67

Критерії вибору методів оцінювання ризиків в задачах інформаційної безпеки *Божаткін С.М.* 73

Аналіз ринку програмних інструментів для оцінювання ризиків інформаційної безпеки *Божаткін С.М.*; *Сірівчук А.С.*; *Турти М.Ю.* 79

Модель процесів інформаційної безпеки на рівні організації *Божаткін С.М.*; *Турти М.В.* 91

Інформаційна модель оцінювання загроз безпеці інформації з обмеженим доступом *Гайванюк І.О.* 95

Врахування підвищення залишкової розбірливості мови в каналі витоку при багаторазовому прослуховуванні *Касьянов Ю.І.*; *Іванова А.В.* 103

Розрахунок бажаних характеристик звукоізоляції та шумової завади за октавними рівнями формантної розбірливості мови *Касьянов Ю.І.*; *Золотченко В.В.* 108

Основні аспекти об'єктивного тонального методу визначення розбірливості мови *Касьянов Ю.І.*; *Трізно С.О.* 113

Визначення ефективності захисту мовної інформації типовими звукоізоляційними конструкціями за їх частотними характеристиками *Кучер В.С.* 119

Дослідження спектрів довготривалих українських мовленнєвих сигналів *Михайличенко А.В.*; *Трощенко С.С.* 124

Інтелектуальні засоби в системах виявлення та запобігання вторгнень *Стефанюк Ю.О.* 129

Інформаційна модель ранжування загроз за BS ISO/IEC 27005:2011 *Турти М.В.*; *Доценко В.В.* 134

Інформаційна модель категоризації об'єктів критичної інфраструктури *Турти М.В.*; *Злочевська О.В.* 140

Інформаційна модель системи визначення оптимальних інвестицій в інформаційну безпеку *Турти М.В.*; *Осипчук А.В.* 147

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2022

X Всеукраїнська науково-технічна конференція
з міжнародною участю

13–14 грудня 2022 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