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

СЕКЦІЯ 4. МОДЕЛЮВАННЯ ОБ'ЄКТІВ І ПРОЦЕСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.5;057.2

АНАЛІЗ ПРОЦЕСУ ІДЕНТИФІКАЦІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

Згідно ISO/IEC 27005:2011 [1] процес оцінки ризиків інформаційної безпеки (РІБ) є ітераційною процедурою і складається з трьох етапів (ідентифікація, аналіз і оцінювання ризику), кожен з яких містить ряд підпроцесів. Кроки ітерації для цього процесу різняться за ступенем деталізації відомостей щодо РІБ, що використовуються на етапі обробки ризиків для визначення комплексу адекватних засобів управління ризиками. При цьому важливою є повнота списків можливих загроз, вразливостей, наслідків успішної реалізації загроз, які формуються на етапі ідентифікації ризиків ІР.

Метою даної роботи є структуризація знань щодо процесу ідентифікації ризиків інформаційної безпеки, для чого необхідно провести аналіз стандартизованого процесу ідентифікації РІБ, визначити структурні компоненти системи знань в цій предметній галузі та їх взаємозв'язки.

Метою ІР є визначення множини потенційно небезпечних для організації подій, їх витоків і наслідків з достатнім для прийняття рішень щодо обробки ризиків ступенем деталізації. До складу процесу ІР ризиків входять, згідно ISO/IEC 27005 п'ять підпроцесів ідентифікації для активів, загроз, засобів контролю, вразливостей і наслідків. На першому кроці ітерації проводиться високорівнева оцінка ризиків за спрощеною процедурою для досягнення субмети – виявлення високих ризиків, інформація щодо яких має бути деталізована. Вхідними даними для ІР є вхідні дані підпроцесу ідентифікації активів, які можуть різнитися на першому і наступних кроках ітерації. На виході процесу ІР в результаті ідентифікації наслідків отримується перелік сценаріїв

інцидентів інформаційної безпеки із визначеними з достатнім ступенем точності ймовірнісними характеристиками та наслідками для окремих активів і бізнес-процесів, що дозволяє провести категоризацію ризиків, визначити прийнятні залишкові ризики, ризики, що не вимагають деталізації і високі ризики, які мають бути деталізовані на наступних кроках ітераційного процесу оцінки РІБ.

Кожен підпроцес процесу ідентифікації РІБ також має власну мету, що підпорядкована цілі процесу ідентифікації РІБ, власні вхідні і вихідні дані та певні принципи проведення. Дерево цілей для процесу ІР наведене на рис.1, а опис вхідних і вихідних даних під процесів разом з визначеними особливостями їх проведення представлені у вигляді табл.1.

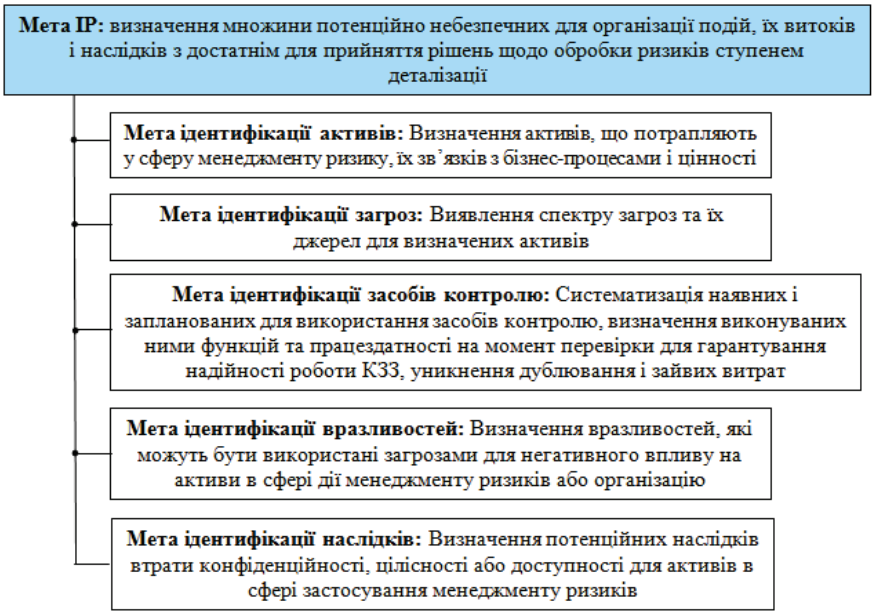

Рисунок 1 – Дерево цілей процесу ідентифікації ризиків

Таблиця 1 – Ідентифікація ризиків

Підпроцес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація активів	Область застосування менеджменту ризиків ІБ, її границя, перелік складових частин із вказівкою їх характеристик, зокрема, функцій, власників, розташування тощо.	Перелік активів, що підлягають менеджменту ризиків ІБ, із визначеною цінністю Перелік пов'язаних з визначеними активами бізнес-процесів із оцінкою їх значимості	Обсяг інформації, що підлягає аналізу, збільшується із поглибленням рівня деталізації Цінність активу найчастіше визначає його власник або особа, що відповідає за отримання, експлуатацію і збереження активу Значимість бізнес-процесів для бізнесу в цілому може визначатися топ-менеджерами
Ідентифікація загроз	Інформація про загрози, отримана при аналізі інцидентів, отримана від власників активів та користувачів, інформація з інших джерел, в тому числі з реєстрів загроз	Перелік загроз із визначеними властивостями (тип загрози, джерело загрози)	Мають бути ідентифіковані випадкові і цілеспрямовані загрози, внутрішні і зовніші загрози, загрози, що впливають на один актив і на декілька активів різним чином тощо. В ідеалі мають бути ідентифіковані всі загрози. Слід враховувати, що спектр значимих загроз постійно змінюється, особливо при зміні інформаційних технологій і бізнес-середовища.

Продовження таблиці 1

Підпроцес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація засобів контролю	Список засобів контролю, план реалізації обробки ризиків, документація на засоби контролю,	Перелік наявних і запланованих для використання засобів контролю із визначенням їх розташування, виконуваних функцій, частоти використання і ефективності	Ефективність засобів контролю кількісно може бути оцінена або шляхом аналізу журналів моніторингу та аудиту, або шляхом експерименту, під час якого визначають на скільки знизилися ймовірність усішної реалізації загрози і легкість використання загрозою сукупності вразливостей. Наявний і запланований для використання засіб контролю може бути ідентифікований як: ефективний; недостатній; неефективний; необґрунтований (економічно недоцільний). Щодо неефективних і недостатніх засобів контролю повинні бути прийняті рішення: про їх видалення і заміну на ефективніші засоби; про введення в КЗЗ додаткових засобів контролю; рішення залишити ситуацію без змін з міркувань вартості

Продовження таблиці 1

Підпроцес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація вразливостей	Перелік активів із визначеною цінністю, перелік загроз із визначенням їх типів та джерел, перелік засобів контролю із визначеною ефективністю	Перелік вразливостей із визначеними їх зв'язками з активами, із загрозами, із засобами контролю Переліки не пов'язаних з загрозою вразливостей для кожної ідентифікованої загрози	Розглядаються вразливості, що є відносно активу: внутрішніми вразливостями зовнішніми вразливостями. Наявність вразливості може бути викликана: порушенням умов експлуатації активу; неефективністю в певних умовах експлуатації засобу контролю. Вразливості можуть ідентифікуватися в таких областях як: організація робіт; прийняті в організації норми управління; процеси і процедури; персонал; фізичне середовище; конфігурація ІКС, апаратні і програмні засоби, засоби зв'язку; зовнішні впливи. Вразливість, яка не експлуатується жодною загрозою: не вимагає впровадження засобів контролю; вимагає проведення моніторингу з метою своєчасного виявлення небезпечних змін. Загроза, яка не має відповідної вразливості, не спричиняє появу ризику.

Продовження таблиці 1

Підпроцес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація наслідків	Перелік активів, перелік бізнес-процесів, перелік загроз, прелік вразливостей із визначеними показниками значимості елементів переліків і їх зв'язками (в разі наявності) з елементами інших переліків.	Перелік сценаріїв інцидентів інформаційної безпеки із визначеними наслідками для активів і бізнес-процесів	Будуються сценарії інцидентів, в яких певна загроза експлуатує певну вразливість. Сценарії можуть будуватися для активу, частини активу, групи активів. Визначаються потенційні збитки від реалізації сценаріїв за всіма критеріями впливу (типами наслідків), прийнятими на етапі визначення контексту. При визначенні операційних наслідків сценаріїв приймають до уваги: час, необхідний для розслідування інциденту; час, необхідний для відновлення системи; втрати ресурсу робочого часу організації внаслідок інциденту; порушення охорони праці і безпеки; втрачені можливості (економічні і неекономічні); фінансові витрати, необхідні для забезпечення специфічних навичок персоналу з ліквідації негативного результату сценарію тощо. Наслідки сценаріїв можуть бути тимчасовими і постійними (приклад – руйнування активу).

Слід зазначити, що реалізація процедур підпроцесів суттєво залежить від типу вхідних і вихідних даних і може здійснюватися на основі різних методів [2, 3].

Висновки

В даній роботі проведено аналіз стандартизованого процесу ідентифікації РІБ, визначені структурні компоненти системи знань в цій предметній галузі та їх взаємозв'язки, зокрема побудовано дерево цілей процесу ідентифікації РІБ, визначені принципи організації підпроцесів процесу ідентифікації РІБ, визначено взаємозалежність вхідних і вихідних даних підпроцесів, що в сукупності являє собою структуру знань щодо процесу ідентифікації ризиків інформаційної безпеки.

Список літератури:

1. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. [URL]: https://www.iso.org/standard/ 56742.html
2. 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.
3. 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.

УДК 004.056.5

КРИТЕРІЇ ВИБОРУ МЕТОДІВ ОЦІНЮВАННЯ РИЗИКІВ В ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: *Божаткін С.М., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Задача оцінювання ризиків є наріжним каменем управління інформаційною безпекою (ІБ). Методологія оцінювання ризиків ІБ стрімко розвивається, зокрема, згідно Плану реалізації Стратегії кібербезпеки України у другому півріччі 2025 року на державному рівні мають бути

ЗМІСТ

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