ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ ВНУТРІШНІХ
СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference "Cybersecurity in Ukraine: Legal and Organizational Issues"

Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року

ОДУВС
м. Одеса
2022

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference "Cybersecurity in Ukraine: Legal and Organizational Issues"

Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року

Одеса
ОДУВС
2022

Рекомендовано до друку рішенням кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання:
К38 матеріали міжн. наук. практ. конф., м. Одеса, 23 листопада 2022 р. Одеса : ОДУВС, 2022. 152 с.
ISBN 678-717-70204

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 23 листопада 2022 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), здобувачам вищої освіти першого та другого півня освіти.

МОДЕЛЮВАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Олексій БАЛТОВСЬКИЙ
професор кафедри кібербезпеки та інформаційного забезпечення ОДУВС, д.т.н., доцент
Олександр ГЕРАСИМЕНКО
слухач магістратури факультету №1 ННІПКБ ОДУВС, спеціальність 124 «Системний аналіз»

Попередній аналіз типових АСУ технологічними процесами (ТП), протоколів передачі інформації та інформаційних ресурсів показує складність їх взаємодій та, як наслідок, потенційну можливість реалізації певних загроз інформаційної безпеки [1, с.44].

Статистику за інцидентами, пов'язаними з порушенням інформаційної безпеки (ІБ), важко зібрати в необхідному обсязі, тому актуальним завданням

є моделювання АСУ ТП з подальшою можливістю оцінювати ризики ІБ, оптимізації витрат, що вимагають підвищення рівня ІБ, та конкретизації рекомендацій до організаційних та технологічних заходів.

Існують різні підходи до моделювання систем захисту інформації (СЗІ), що відбивають різні аспекти систем захисту [1, с.48]:

− моделі, що використовують підходи теорії ймовірності та нейронних мереж;

− моделі, побудовані з використанням теорії мереж Петра-Маркова;

− моделі, що ґрунтуються на теорії кінцевих автоматів;

− моделі, збудовані з використанням теорії графів;

− моделі, що використовують теорію нечітких множин;

− моделі, збудовані з використанням ентропійного підходу; − теоретико-множинні моделі.

Моделі, що використовують теорію ймовірності та нейронні мережі, ідеально працюють, наприклад, при аналізі аномалій мережевого трафіку із зовнішньої мережі, коли можна на основі статистики класифікувати аномалію та прийняти рішення про блокування певного трафіку.

Моделі на основі мереж Петра-Маркова, як і моделі, що використовують автомати Мура, добре зарекомендували для аналізу управління ймовірністю успішної реалізації несанкціонованого доступу за часом (з використанням статичних даних).

Моделі ІБ, що використовують теорію графів, добре працюють у системах підтримки прийняття рішень з використанням експертів, коли, наприклад, необхідно оцінити безпеку певного шляху реалізації процесу, а для оптимізації вибору найбезпечнішого маршруту використовується модифікований алгоритм Дейкстри.

Моделі з урахуванням нечітких множин (модель Мамдані, TSK-моделі та інших.) можна використовуватиме оцінки ризиків ІБ з допомогою добре спланованих експериментів та експертів, здатних грамотно оцінити результат роботи моделі, тобто. отриманий ризик, за вхідними даними. Зазвичай добре працюють для конкретних інформаційних процесів в захищеної інформаційній системі (ІС).

Моделі ІБ, побудовані з урахуванням ентропійного підходу, використовуються виявлення можливості ідентифікації користувачів веб-ресурсів [1, с.67].

Теоретико-множинний опис представляє універсальну модель, т.к. може бути застосована до широкого класу систем [1, с.67].

Як правило, підхід до моделювання вибирають, орієнтуючись на параметри, що використовуються як вхідна інформація, та результати розрахунків, які отримані на виході. Зазвичай вхідна інформація базується на наявній статистиці для існуючих ІС та/або даних експертів. Модель, що розробляється, повинна містити формальний опис об'єкта моделювання, що враховує відносини між елементами ієрархічної структури АСУ ТП. Так як описані види моделей ефективні для певних завдань з недоглядами, а в даному випадку відсутня можливість визначити зв'язок або характер залежності, то на першому етапі необхідним є використання теоретико-множественної моделі.

Також модель, що розробляється, не повинна пропонувати конкретних результатів, вона надає можливість відстежити взаємодію активів,

Таким чином, пропонована модель використовуватиме теоретичній підхід, саме у такому вигляді зручно формалізувати концептуальне опис системи, т.к. концептуальна модель зрештою представляє опис певної структури взаємопов'язаних понять та відносин між ними.

Для автоматизації технологічних процесів використовуються АСУ ТП, побудовані з урахуванням програмованого логічного контролеру (ПЛК) та пристрою зв'язку з об'єктом (ПЗО) [2, с.34]. Одним із завдань коректного функціонування АСУ ТП є забезпечення ІБ цих систем.

Важливо відзначити уявлення, що функціонування АСУ ТП складно порушити через такі обставини:

− ПО кожній АСУ ТП, як правило, пропрієтарне та закрите [2, с.35];

− у локальній мережі користувачів на верхньому рівні АСУ ТП проблеми з безпекою можна вирішити організацією коректної політики обмеження доступу;

− проникнення в АСУ ТП пов'язані з великими інтелектуальними витратами, а вигода для зловмисника очевидна [2, с.30].

Однак інциденти, пов'язані із зараженням АСУ ТП промислових підприємств такими шкідливими програмами як Stuxnet [2, с.34], Duqu [2, с.34], Flame [2, с.34], WannaCry [2, с.35] та іншими, свідчать про інше. Більше того, факт, що підприємства передають дані до зовнішніх мереж, наприклад, до центрального офісу, показують, що такі системи необхідно захищати, в т.ч. через можливе використання інформаційних технологій як інструменту тиску та протиборства. Це знайшло відображення у Стратегії національної безпеки США 2015 року.

Необхідно відзначити, що атакам піддаються не тільки пристрої верхнього рівня, але також пристрої середнього та нижнього рівня [27,99]. Це змушує по-новому порушити питання, пов'язані з ІБ підприємств, які використовують АСУ ТП.

Об'єднання пристроїв у мережу, наявність з'єднань між різними зонами, а також поява інтерфейсів для віддаленого обслуговування створюють умови, за яких виникають загрози ІБ для АСУ ТП та підприємства в цілому.

Враховуючи, що АСУ ТП критичної інфраструктури (КІ) є суб'єктами критичних інформаційних інфраструктур (КІ), до систем автоматизації таких підприємств висуваються підвищені вимоги щодо забезпечення стабільності роботи процесів та надійності їх функціонування. Подібні вимоги обумовлюють наявність особливого підходу до оцінки ризиків під час побудови та підтримки системи захисту інформації АСУ ТП від загроз ІБ.

За відсутності адекватної оцінки ризиків складно відповісти на питання про початок побудови системи захисту інформації, необхідні ресурси, види загроз, від яких слід захищати, про типи достатніх і пріоритетних контрзаходів [2, с.55]. Складно також вирішувати завдання оцінки необхідності та достатності певного набору контрзаходів, їхньої адекватності існуючим ризикам

[2, с.55]. Таким чином, завдання оцінки ризиків, пов'язаних із здійсненням атак на АСУ ТП, є першочерговим.

Література:

1. Захист інформації в автоматизованих системах управління: навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. Житомир: Вид-во ЖДУ ім. І. Франка, 2018. 226 с.

2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. К.: ДУТ-КНУ, 2016. 178 с.