Щербина Юрій Володимирович

Національний університет «Одеська юридична академія»,

доцент кафедри інформаційних технологій, кандидат технічних наук, доцент

Єфремов Владислав Анатолійович

Національний університет «Одеська юридична академія»,

студент факультету кібербезпеки та інформаційних технологій

АКТУАЛЬНІ ПИТАННЯ ТА ПРОБЛЕМИ ЗАХИСТУ СУЧАСНОГО КІБЕРПРОСТОРУ

Втілення кіберфізичних систем (Cyber-Physical System, CPS) у сучасне виробництво та процеси, пов’язані з управлінням складними технологічними процесами, приводять до кардинальних змін у суспільстві. Вони будуються на базі природних об’єктів та інтелектуальних мереж (Smart Grid), що використовуються для підвищення ефективності автоматизації управління інфраструктурою енергопостачання, телекомунікаційних та оборонних систем та їм подібних [1]. CPS відносять до складу великих складних системах, у яких відбувається збір та оброблення великих потоків інформації, а також моніторинг стану технологічного обладнання. На жаль, крім переваг, що дає використання інтелектуальних технологій, цифровізація виробництва, суспільного життя, і бізнесу виникає віртуальний простір для скоєння кіберзлочинів. Із цього факту логічно витікає необхідність постійного проведення досліджень пов’язаних із реагуванням на події у середовищі експлуатації, що викликають необхідність відновлення ресурсів, та нормального стану інформаційних процесів.

Кіберзлочини, на відміну від інформаційних злочинів, мають на меті порушення нормального функціонування процесів управління інфраструктурними об’єктами, завдання економічних збитків конкурентам, внесення порушень у виробничі процеси або підготовку і скоєння терористичних атак.

Проблема попередження подібних дій ускладнюється надзвичайною розподіленністю, інтелектуальних інформаційно-телекомунікаційних мереж. Складність їх архітектури та апаратного забезпечення збільшує ймовірність потенційно можливих мережевих атак на критично важливі процедури управління та обчислювальні ресурси. Через це, очевидною є важливість постійного моніторингу ризиків у середовищі експлуатації кіберфізичних систем та своєчасне запобігання зовнішнім втручанням [2].

Оскільки наслідками кібератак можуть бути події, що утворюють загрози життю людей, виникненню техногенних катастроф а також великих матеріальних втрат, системи кібербезпеки повинні зменшувати ризики реалізації загроз, виявляти та ідентифікувати аномальну поведінку системи, а також оперативно відновлювати нормальний стан системи.

Актуальні атаки на кіберфізичні системи

Комп'ютерна злочинність виникла майже одночасно із появою відкритої колективної обчислювальної мережі та розподілених обчислювальних процесів. Зростання кола послуг, що Internet надає своїм користувачам лише ускладнює цю проблему. Наприкінці 1999 року у світ вийшли «Загальні критерії», прийняті в Україні як ДСТУ ISO/IEC 15408:2017 [3]. Разом з іншими суміжними документами, вони визначали термінологію та засади захисту інформації у відкритому мережевому просторі. Питання управління та організації захисту вперше були викладені у стандарті BS 7799, виданому Британським інститутом стандартів (British Standards Institution – BSI) під назвою «Практичні правила управління інформаційною безпекою» у 1995 році. Після 2000 року на його основі ISO/IEC JTC 1/SC 27 випускав міжнародні стандарти серії ISO/IEC 27000, де визначається модель та функції управління безпекою. Вони є результатом консенсусу, згоди і накопиченого досвіду експертів різних країн.

З урахуванням зміни, що відбулися загальному інформаційному просторі, ISO/IEC оприлюднило новий міжнародний стандарт ISO/IEC 27032:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови із кібербезпеки» [4]. У цьому стандарті було визначено такі поняття як кіберпростір та кібербезпека і надано їх тлумачення. Кіберпростір визначається

як комплексне віртуальне середовище, яке виникає під час взаємодії людей, програмного забезпечення та Internet-послуг, що підтримуються міжнародними розподіленими фізичними інформаційно-телекомунікаційними технологіями та мережами зв’язку. Не зважаючи на його “віртуальність” сплановані у ньому атаки на ресурси кіберфізичних систем можуть викликати економічний колапс, паралізувати оборонні структури, або значно знизити ефективність управління державними органами. Ще два десятиріччя тому головними задачами захисту були збереження конфіденційності та цілісності даних, то сьогодні мова іде про кібернетичну війну і кібернетичну зброю.

Одним із серйозних видів, актуальних на даний час кібернетичних атак, розглядається атака повторного відтворення (Replay attacks). Її ціллю є система автентифікації. Шляхом запису і подальшого відтворення коректного повідомлення або його частини [5] в систему вводяться хибні дані. Для імітації автентичності вона використовує будь-яку незмінну інформацію, наприклад, пароль або біометричні дані. Паралельно із цією атакою зловмисники використовують атаку червоточини (Wormhole attack). Вони перехоплюють інформацію між двома кінцевими точками і передають її іншим суб’єктам, створюючи таким чином “тунель” контролю.

Іншою, поширеною і небезпечною у кібернетичному просторі атакою, є атака, обману (Deception attacks). Її ціллю є втручання у фізичні і кібернетичні процеси через системи телекомунікації для отримання контролю над окремими її частинами [6]. Обман може бути визначений як взаємодія між двома суб'єктами – суб’єктом, що є джерелом атаки і суб’єктом-ціллю. Джерело атаки намагається змусити ціль прийняти неправдиву версію дійсності, бажану обманщикові.

На відміну від природного середовища, канали зв'язку у кіберпросторі несуть менше інформації, ніж канали при звичайній взаємодії суб'єктів, а інформація у кіберпросторі схильна до постійних змін. Обидва ці фактори сприяють реалізації шахрайських дій. Тому атаки обману не мають окремої типової моделі. Їх сценарії визначаються в залежності від поставлених цілей, вразливостей і наявних ресурсів порушників безпеки. У разі нападу на технологічні системи, основними цілями атак обману є маніпуляції із

показаннями датчиків, підробка керуючої інформації та отримання доступу до важливих ресурсів систем.

По мірі розвитку систем кібернетичного захисту будуть вдосконалюватися і сценарії нападу на критично важливі об’єкти кіберфізичних систем.

Сьогодні існує велика кількість методів виявлення і зупинення атак такого типу. Через це, для організації надійного захисту необхідним є постійний моніторинг мережевих подій, вивчення вразливостей системи та сценаріїв атак, що мали місце раніше, їх оцінка і пошук способів ефективної протидії а також створення відповідних експертних систем [7].

Протидія кіберзлочинності ґрунтується на створенні їх математичних моделей, які на формальному рівні описують сценарії мережевих атак, головною з яких є модель DoS-атаки, побудованої на основі схеми Бернуллі. Вхідними даними для неї є результати моніторингу вторгнень у кіберфізичний простір та накопичений досвід в організації протидії зовнішнім втручанням.

Складність проблеми пояснюється динамічністю поведінки складових частин кіберфізичних систем, а також тим, що передбачити можливі сценарії атак у кіберпросторі майже неможливо. Ця задача ще чекає свого ефективного вирішення. Вона не є цілком технічною, оскільки порушникам не завжди володіють всією необхідною для організації атак інформацією, вони вимушені користуватись ще й агентурними методами.

Виходячи із цього, захисники мереж зі свого боку повинні вирішувати проблему багатоцільової оптимізації. Це складна задача, але її вирішення у даний момент виглядає дуже важливим.

Список використаних джерел:

1. Janssen M.C. The Smart Grid Drivers, PAC World, 2010, 77 p.

2. National Institute of Standards and Technologies (NIST): ‘Guidelines for smart grid cybersecurity’ (NIST Special Publication, Gaithersburg, MD, 2014). Available at url: http://www.dx.doi.org/10.6028/NIST.IR.7628r1

3. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT)

4. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for Cybersecurity. – 2012-07

5. Dutt, V., Ahn, Y. S., & Gonzalez, C.: Cyber situation awareness modeling detection of cyber-attacks with instance-based learning theory. Human Factors: The Journal of the Human Factors and Ergonomics Society, 55(3), 605-618 (2013).

6. D. Ding, Z. Wang, Q.-L. Han, G. Wei, Security control for a class of discretetime stochastic nonlinear systems subject to deception attacks, IEEE Trans. Syst. Man Cybern.Syst. doi:10.1109/TSMC.2016.2616544.

7. Sridhar, S., Govindarasu, M.: 'Model-based attack detection and mitigation for automatic generation control', IEEE Trans. Smart Grid, 2014, 5, (2), pp. 580–591.

Ключові слова: кіберпростір, кіберфізичні система, кібератака, кібербезпека.

Ключевые слова: киберпространство, киберфизическая система, кібератака, кибербезопасность.

Keywords: cyberspace, cyberphysical system, cyberattack, cybersecurity.

Колосенко Андрій Андрійович

Національний університет «Одеська юридична академія»,

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій

ІНСТИТУТ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА ЯК ОДИН З МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

У часи невпинного технічного прогресу, діяльність держави, підприємств та організацій нерозривно пов'язана з інформаційно-комунікаційними технологіями.