2016. – V. 2. – No 2 (2). – P. 61 -63.
5. *Chris Clymer, Ken Stasiak, Matt Neely, Stephen Marchewitz.* IRisk Equatuion [Електронний ресурс] – Режим доступу: https://securestate.en/iRisk-Equation-Whitepaper.pdf
6. Common Vulnerability Scoring System v3.0: User Guide [Електронний ресурс] – Режим доступу: https://www.first.org/cvss/user-guide
7. Cisco IOS Software Command Authorization Bypass [Електронний ресурс] – Режим доступу: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328pai
8. Cisco Web Security Appliance Administrative Interfaces Access Control Bypass Vulnerability [Електронний ресурс] – Режим доступу: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa5
9. Эксплойт EternalBlue [Електронний ресурс] – Режим доступу: https://habrahabr.ru/company/panda/blog/329044
10. Meltdown [Електронний ресурс] – Режим доступу: https://meltdownattack.com/meltdown.pdf
11. Spectre Attacks: Exploiting Speculative Execution [Електронний ресурс] – Режим доступу: https://spectreattack.com/spectre.pdf

Поступила 19.02.2018р.

УДК 519.711

Д.В. Савельєв, Київ

МОДЕЛЬ ЗАГРОЗ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ У СФЕРІ ЯДЕРНОЇ ЕНЕРГЕТИКИ

Abstract. The article describes the process of constructing a model of cybersecurity threats, contains a list of possible cybersecurity threats of critical information infrastructure objects in the nuclear power industry, describe the possible consequences of implementing each type of threats.

Вступ

Міжнародні організації, такі як Міжнародне агентство з атомної енергії (МАГАТЕ), Міжнародна електротехнічна комісія (МЕК), а також національні органи регулювання ядерної та радіаційної безпеки різних країн працюють над питанням вивчення та регулювання інформаційної безпеки АЕС, що викликано трьома основними факторами – масовою тенденцією переходу від аналогових до цифрових інформаційних та керуючих систем АЕС, вразливістю таких систем до кіберзагроз та підвищенням кількості випадків зловмисних дій щодо інформаційних систем з серйозними наслідками [1].

Забезпечення інформаційної безпеки є важливим завданням, адже

кібератаки на об’єкти критичної інформаційної інфраструктури сфери ядерної енергетики можуть негативно вплинути на фізичну безпеку, і в наслідок – ядерну та радіаційну безпеку АЕС та інших ядерних установок.

Однією з основних задач забезпечення інформаційної безпеки є визначення переліку загроз та оцінка ризиків їх впливу, що дозволяє визначити склад системи захисту інформації.

У даній статті розглядаються питання побудови моделі загроз кібербезпеки, приводиться перелік можливих типів загроз кібербезпеки об’єктів критичної інформаційної інфраструктури у сфері ядерної енергетики, вказано можливі наслідки реалізації для кожного типу загроз.

Основна частина

Модель загроз містить систематизований перелік загроз безпеки даних при їх обробці в інформаційних системах. Ці загрози зумовлені умисними чи ненавмисними діями зловмисників, обслуговуючого персоналу та користувачів системи, які можуть мати серйозні негативні наслідки.

Модель загроз кібербезпеки об’єктів критичної інформаційної інфраструктури у сфері ядерної енергетики (далі – Об’єкти) містить єдині початкові дані по загрозам безпеки даних, які обробляються на Об’єктах, пов’язані з:

- перехопленням даних по технічним каналам з метою їх копіювання чи неправомірного розповсюдження;
- несанкціонованим, в тому числі випадковим, доступом до Об’єкта з метою змінення, копіювання, розповсюдження або деструкційного впливу на його елементи та оброблювані дані з використанням програмних та програмно-апаратних засобів з метою знищення або блокування.

Модель загроз є методичним документом, із застосуванням якого вирішуються наступні задачі:

- аналіз захищеності Об’єкта від загроз кібербезпеки в ході організації та виконання робіт по забезпеченню його безпеки;
- розробка системи захисту даних, яка забезпечує нейтралізацію можливих загроз з використанням методів та засобів захисту даних, передбачених для відповідного типу Об’єкта;
- проведення заходів, націлених на запобігання несанкціонованого доступу до даних, впливу на технічні засоби Об’єкта, який призведе до порушення їх функціонування;
- контроль забезпечення рівня захищеності Об’єкта.

Первинний перелік загроз формується комбінаціями можливих факторів, впливаючих на інформацію, що потребує захисту, категоріями засобів захисту та рівнями впливу порушників.

Виявлення та врахування факторів, що впливають або можуть впливати на інформацію в конкретних умовах, формують основу для планування та

проведення ефективних заходів, що забезпечують захист інформації об'єктів критичної інформаційної інфраструктури. Повнота та достовірність виявлення факторів досягається розглядом повного переліку факторів, які впливають на усі елементи об'єкта критичної інфраструктури на усіх етапах обробки інформації. У матеріалі [2], де описується методика побудови моделі загроз безпеки інформації для автоматизованих систем, також описується та наводиться ER-модель бази даних моделі загроз.

Формування вторинного переліку загроз відбувається завдяки доповненню на основі статистики про інциденти та виходячи з умов ступеня їхнього деструктивного впливу, який може визначатись:

- імовірністю виникнення загрози;
- втратами внаслідок реалізації загрози;
- часом на відновлення системи.
- Деструктивний вплив може призвести до:
- порушення конфіденційності інформації;
- несанкціонованого впливу на вміст інформації, її модифікації чи руйнування;
- несанкціонованого впливу на програмні елементи інформаційної системи з подальшим блокуванням інформації;
- втрати автентичності даних;
- втрати достовірності систем.

Міра ризику, яка дозволяє проаналізувати та структурувати загрози за пріоритетністю, може бути визначена як загальні збитки від кожного виду проблем.

Результатом оцінки ризику виникнення кожної загрози повинні бути:

- комплексне застосування відповідних засобів захисту інформації;
- прийняття ризиків, яке забезпечує цілковите заохочення вимог політик інформаційної інфраструктури та їх критеріїв прийняття ризиків;
- максимально можлива відмова від ризиків виникнення загроз.

Кібератаки, віруси, шкідливе програмне забезпечення (далі – ПЗ), несанкціоновані модифікації ПЗ та даних є загрозою для Об’єктів, оскільки можуть небезпечно впливати на їх функціонування та технологічні процеси, що реалізовуються під їх керуванням. Базова класифікація зловмисних дій, які застосовуються до Об’єктів та стосуються фізичної, ядерної та радіаційної безпеки, наведена у положенні МАГАТЕ [3]:

- атаки для збору інформації з метою планування та здійснення подальших злочинних дій;
- атаки, направлені на відключення або погіршення роботи однієї чи декількох систем (інформаційної та керуючої системи, технічних засобів) разом з іншими паралельними режимами атаки, такими як фізичне вторгнення на ядерну установку;
- порушення нормальної роботи однієї чи декількох систем (інформаційної та керуючої системи, технічних засобів) у поєднанні з

іншими паралельними режимами атаки, такими як фізичне вторгнення на ядерну установку.

За результатами аналізу, виконаного Державним підприємством «Державний науково-технічний центр з ядерної та радіаційної безпеки» (ДНТЦ ЯРБ), у публікації [1] пропонується виділити дві великі групи кібернетичних загроз:

- кібернетичні загрози на стадії розробки інформаційних та керуючих систем;
- кібернетичні загрози на стадії експлуатації інформаційних та керуючих систем на Об'єктах.

В наведених групах можна виділити декілька основних типів кібернетичних загроз за способом впливу на Об'єкти.

До першої групи можна віднести наступні можливі типи загроз:

- шкідливі закладки в ПЗ власної розробки – шкідливий програмний код може бути доданий будь-ким з команди розробників, тому слід максимально контролювати процес розробки ПЗ на усіх стадіях (важливо враховувати, що до складу однієї системи може входити ПЗ різних класів безпеки, та можливий негативний вплив ПЗ більш низького класу на ПЗ більш високого класу безпеки);
- шкідливі закладки в придбаному ПЗ – використовуючи готовий продукт розробник інформаційної та керуючої системи не може контролювати процес розробки ПЗ на усіх стадіях (ймовірність наявності шкідливих закладок у такому ПЗ не виключається);
- негативний вплив на ПЗ Об'єктів з боку засобів розробки ПЗ – різні засоби розробки ПЗ можуть формувати некоректний вихідний чи виконуваний програмний код через ненавмисні внутрішні помилки в цих засобах, або в результаті умисного закладених в них шкідливих функцій (необхідний контроль коректності функціонування таких засобів та детальна перевірка автоматично генерованого коду);
- загрози об'єктно-орієнтованого програмування – при застосуванні об'єктно-орієнтованого програмування для розробки ПЗ інформаційних та керуючих систем необхідно враховувати, що у програмному коді, як правило, буде використано значну кількість стандартних об'єктів, запропонованих мовою програмування (теоретично, код стандартних об'єктів може містити команди, які за певних умов можуть негативно вплинути на роботу системи);
- закладки в технічних засобах – такі закладки являють собою шкідливі та приховані модифікації електронних пристроїв, та можуть змінювати функціонування модулів, які містять програмні компоненти або базуються на технології програмованих логічних інтегральних схем, що приводить до порушення їх роботи та може негативно впливати на роботу системи (детальний аналіз закладок у технічні засоби наведено у [4]).

Кібернетичні загрози на стадії експлуатації інформаційних та керуючих систем на Об'єктах включають шкідливі впливи, які реалізовуються у процесі експлуатації та негативно впливають на функціонування систем. На цій стадії можна виділити наступні типи загроз:

- негативний вплив через мережі передачі даних – впровадження вірусів, не направлених на конкретну систему, або цілеспрямовані атаки на конкретну інформаційну та керуючу систему чи Об'єкт;
- внесення шкідливих програм чи даних з портативних пристроїв, або із зовнішніх накопичувачів даних у ході експлуатації;
- негативний вплив з боку контрольно-перевірної апаратури – контрольно-перевірна апаратура слугує потенційним джерелом шкідливого впливу на системи, важливі для безпеки Об'єктів (дана апаратура підключається до систем у ході їх випробувань, відновлення чи технічного обслуговування);
- шкідливі дії, виконуванні безпосередньо обслуговуючим персоналом Об'єктів чи сторонніми організаціями – такі дії можуть бути як ненавмисними, так і умисними (умисні, в свою чергу, можуть у результаті бути як дрібна шкода чи саботаж конкретного співробітника, так і добре спланована диверсія);
- модифікація інформації, що надходить від датчиків – некоректна інформація, що надходить від датчиків, може привести до порушення технологічного процесу;
- некоректне оновлення ПЗ, що використовується на Об'єктах – при доопрацюванні, модифікації чи оновленні ПЗ існує ризик внесення у систему шкідливого ПЗ чи ненавмисних помилок.

У табл. 1 приведено можливі наслідки від реалізації описаного переліку видів загроз.

Таблиця 1

Можливі наслідки реалізації загроз

Група кібернетичних загроз	Можливі типи загроз	Можливі наслідки реалізації загрози
Загрози на стадії розробки інформаційних та керуючих систем	Шкідливі закладки у ПЗ власної розробки	Виконання будь-яких деструктивних дій
	Шкідливі закладки у придбаному ПЗ	Виконання будь-яких деструктивних дій; отримання несанкціонованого доступу
	Негативний вплив на ПЗ з боку засобів розробки ПЗ	Порушення функціонування, можливий деструктивний вплив на систему
	Загрози об'єктно-орієнтованого програмування	Можливий негативний вплив з боку коду стандартних об'єктів за певних умов на роботу системи

	Закладки в технічних засобах	Порушення функціонування, негативний вплив на роботу системи
Загрози на стадії експлуатації інформаційних та керуючих систем на Об'єктах	Негативний вплив через мережі передачі даних	Порушення конфіденційності, цілісності та доступності даних; приховане керування системою; порушення працездатності мережних пристроїв
	Внесення шкідливих програм чи даних із зовнішніх пристроїв	Порушення конфіденційності, цілісності та доступності даних; виконання будь-яких деструктивних дій
	Негативний вплив з боку контрольно-перевірочної апаратури	Можливий негативний вплив на роботу системи
	Шкідливі дії обслуговуючого персоналу Об'єктів чи сторонніх організацій	Виконання будь-яких деструктивних дій
	Модифікація інформації, що надходить від датчиків	Порушення технологічного процесу
	Некоректне оновлення ПЗ	Внесення у систему шкідливого ПЗ чи ненавмисних помилок

Представлений у публікації [1] перелік видів загроз не є повним та в подальшому може розширюватись або бути уточненим. Виконаний авторами [4] аналіз показує основні можливі шляхи кібернетичних атак та дозволяє оцінити важкість захисту від усіх можливих загроз.

Висновки

Забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури у сфері ядерної енергетики актуальні в багатьох країнах. Побудова моделі загроз інформаційної безпеки є однією з основних задач при визначенні складу системи захисту інформації.

Проведено опис моделі загроз, як методичного документа, із застосуванням якого вирішуються задачі аналізу захищеності Об'єктів, розробки системи захисту інформації, проведення заходів щодо запобігання несанкціонованого доступу до даних та впливу на технічні засоби, контролю забезпечення рівня захищеності Об'єктів. Визначено порядок формування переліку загроз кібербезпеки, мір ризику для аналізу та структурування загроз за пріоритетністю для формування результату оцінки ризику виникнення кожної загрози.

Наведено базову класифікацію зловмисних дій, які застосовуються до Об'єктів та стосуються фізичної, ядерної та радіаційної безпеки, відповідно до положення МАГАТЕ [3]. Сформовано перелік основних груп кібернетичних загроз та можливих типів загроз за способом впливу на

Об'єкти за результатами аналізу, наведеного у публікації [1].

Методики побудови моделі загроз, у тому числі розглянута методика у публікації [2], можуть стати основою для розробки універсальних алгоритмічних та математичних моделей безпеки, які ефективно поєднують у собі вимоги нормативно-методичних документів, методологію побудови моделі загроз, моделей порушення і т.д.

1. *Клевцов А.Л.* Компьютерная безопасность информационных и управляющих систем АЭС: кибернетические угрозы / А.Л. Клевцов, С.А. Трубчанинов // Ядерна та радіаційна безпека. – 2015. – №. 1 (65). – С.54-58.
2. *Бондарь И.В.* Методика построения модели угроз безопасности информации для автоматизированных систем / И.В. Бондарь // Сибирский журнал науки и технологий. – 2012. – № 3 (43). – С.7-10.
3. Computer security at nuclear facilities: reference manual: technical guidance. – Vienna: International Atomic Energy Agency, 2011. – (IAEA nuclear security series, ISSN 1816-9317; No. 17). – ISBN 978-92-0-120110-2.
4. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security / Edited by Yastrebenetsky M., Kharfchenko V. – USA, Hershey, IGI Global, 2014. – 450 p.

Поступила 26.02.2018р.

УДК 519.6:504.064

В.О. Артемчук, Київ
І.П. Каменева, Київ
А.В. Яцишин, Київ
Т.М. Яцишин, Івано-Франківськ

МЕТОДИЧНІ ТА ІНФОРМАЦІЙНІ ЗАСОБИ АНАЛІЗУ ЕКОЛОГІЧНИХ РИЗИКІВ НА ОСНОВІ ДАНИХ МОНІТОРИНГУ

Abstract. We consider a general approach to the determination of risks of various origins, based on probabilistic assessments of the behavior of complex systems. To determine the potential risk for the atmospheric factor, an algorithm for estimating the territorial distribution of risks has been developed. Within the framework of the proposed approach, information-analytical, algorithmic and software tools for the analysis of environmental risks have been developed.

Вступ. Розвиток суспільства на сучасному етапі все більше залежить від вирішення проблем екологічної безпеки, захисту людини і довкілля від надмірного техногенного впливу. Стійкий розвиток і безпека визначають дві взаємопов'язані тенденції, що мають вирішальне значення при виборі цілей і шляхів переходу до гармонійної взаємодії природи і суспільства [1, 2].

