COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.081

УДК 004.056

ПІДХОДИ ДО МОДЕЛЮВАННЯ ЗАГРОЗ ПІД ЧАС СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ БАГАТОРІВНЕВИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ КЕРУВАННЯ

Т. Б. Крет

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: taras.b.kret@lpnu.ua

Розглянуто проблему моделювання загроз під час створення комплексної системи захисту інформації в багаторівневих інтелектуальних системах керування. Описано наявні підходи до створення моделі загроз. Запропоновано розглядати багаторівневу інтелектуальну систему керування як різновид автоматизованої системи згідно з класифікацією української нормативної документації. Проведено аналіз процесу створення моделей загроз для автоматизованих систем.

Для вибору оптимальної методики створення моделі загроз у багаторівневих інтелектуальних системах керування було досліджено методики (фреймворки), які можуть бути використані під час моделювання загроз: MITRE ATT&CK, Cyber Kill Chain by Lockheed Martin.

На основі порівняльного аналізу обґрунтовано застосування методики MITRE ATT&CK як найефективнішого методу для моделювання загроз у багаторівневих інтелектуальних системах керування.

Ключові слова: модель загроз, комплексна система захисту інформації, багаторівнева інтелектуальна система керування, MITRE ATT&CK, Cyber Kill Chain by Lockheed Martin, КСЗІ, БІСК.

Вступ

У цій роботі запропоновано підходи до побудови моделі загроз під час розробки комплексної системи захисту інформації (КСЗІ) для багаторівневих інтелектуальних систем керування (БІСК) та обрано найефективніший з них. БІСК – один із різновидів застосування інтелектуальної системи до процесу керування складним об'єктом. Інтелектуальні системи поширені у різних сферах господарської діяльності, що зумовлено їх здатністю до розв'язування неформалізованих задач. Прикладами реалізації БІСК є "розумні" будинки/міста, автономні автомобілі, промислові роботи, тобто системи, які на основі аналізу отриманої інформації з давачів здатні приймати рішення на керування без участі людини. Механізми ухвалення рішень на виконання дій у таких системах формуються на основі методів штучного інтелекту, експертних систем, нейронних мереж тощо.

Архітектурно такі системи складаються з давачів, виконавчих механізмів, блоків керування та комунікаційних мереж, які пов'язують ці елементи між собою. Треба зазначити, що в таких системах блоки керування можуть бути інтегровані у виконавчі механізми або давачі та приймати рішення на виконання самостійно в межах свого рівня.

Моделювання загроз є першочерговим та важливим етапом під час створення КСЗІ. З огляду на це доцільно проаналізувати наявні підходи до моделювання загроз та обрати найефективніший для БІСК з огляду на особливість даних систем – інтелектуальні механізми прийняття рішень, розподіленість та багаторівневість.

1. Огляд літературних джерел

З огляду на складну архітектуру БІСК, зловмисники можуть атакувати будь-який з рівнів системи, чим порушувати роботу як окремого рівня, так і системи загалом. Тому захист має ґрунтуватись на комплексному багаторівневому підході з врахуванням кращих практик та стандартів у галузі інформаційної безпеки [1, 2]. Одним з таких підходів є побудова КСЗІ, яка містить організаційні дії та інженерно-технічні плани, а також апаратно-програмні рішення, що в комплексі забезпечують безпеку інформації в автоматизованій системі (АС) [3].Згідно з НД ТЗІ 2.5-005-99 АС поділяють на три класи [4]:

Клас 1 – одномашинний однокористувачевий комплекс:

- обробляє інформацію однієї або кількох категорій конфіденційності;
- дає можливість працювати лише одному користувачу;
- наприклад – комп’ютер / робоча станція тощо.

Клас 2 – локалізований багатомашинний багатокористувачевий комплекс:

- обробляє інформацію різних категорій конфіденційності;
- має користувачів з різними повноваженнями;
- наприклад – локальна обчислювальна мережа.

Клас 3 – розподілений багатомашинний багатокористувачевий комплекс:

- обробляє інформацію різних категорій конфіденційності;
- потребує передання інформації через незахищене середовище;
- наприклад – глобальна мережа.

Ці класи дають можливість визначити різні види АС залежно від їхнього призначення та функцій. З огляду на це, БІСК можна розглядати як АС 2-го або 3-го класу залежно від типу комунікаційної мережі (локальна, глобальна), через яку взаємодіють її елементи.

Першочерговими етапами побудови КСЗІ для БІСК як АС є [5]:

1. Аналіз об’єкта захисту та моделювання загроз.

На цьому етапі треба визначити ресурси АС, що підлягають захисту, і можливі загрози для них, оцінити їх ймовірність і величину збитків.

2. Оцінка ризиків.

Полягає у визначенні рівня ризику для кожного ресурсу і загрози, враховуючи наявні вразливості і заходи захисту, і виразити його в грошовому або формальному вимірі.

3. Вироблення заходів захисту.

Треба розробити заходи захисту, які дадуть можливість знизити рівень ризику до прийнятного рівня і сформулювати або скоригувати політику безпеки.

4. Розробка плану захисту.

Відображає послідовність усього життєвого циклу комплексної системи захисту інформації, що відповідають стадіям і етапам життєвого циклу АС, і дає можливість оцінити вартість захисту системи.

З огляду на літературні джерела [6, 7], моделювання загроз є актуальним та важливим етапом для побудови КСЗІ, а проблематика

2. Мета та постановка завдання

Ця стаття присвячена аналізу підходів, які можна використати до моделювання загроз під час створення комплексної системи захисту інформації для багаторівневих інтелектуальних систем керування.

Постановка завдання:

- запропонувати використання методик дій порушників під час моделювання загроз у БІСК;
- проаналізувати процес створення моделі загроз для БІСК;
- порівняти методики Cyber Kill Chain від компанії Lockheed Martin та ATT&CK від компанії MITRE для їх використання під час моделювання загроз для БІСК;
- після проведеного аналізу зробити висновок щодо доцільності використання однієї з методик для моделювання загроз під час створення КСЗІ в БІСК.

3. Етапи створення моделі загроз у БІСК

Загальний процес створення моделі загроз описано в Типовому положенні про службу захисту інформації в автоматизованій системі. Цей процес поділяють на такі етапи, де визначаються [8]:

1. Способи реалізації загроз, а саме:

1.1 – технічні канали: побічні електромагнітні випромінювання та наведення, акустичні, оптичні, радіо- та радіотехнічні канали тощо;

1.2 – канали спеціального впливу: формують поля і сигнали для знищення чи порушення конфіденційності, цілісності або доступності інформації;

1.3 – несанкціонований доступ: передбачає під'єднання до апаратури та ліній зв'язку без дозволу; підлаштування під зареєстрованого користувача; обхід заходів захисту для використання інформації або підстановка недостовірної інформації; застосування пристроїв-закладок чи програм-закладок та впровадження комп'ютерних вірусів.

2. Основні види загроз, які можуть бути реалізовані, наприклад: зміна умов фізичного середовища; збої і відмова в роботі; наслідки помилок під час проєктування; помилки персоналу; навмисні ді.

3. Перелік загроз та їх класифікація за впливом на інформацію, тобто спрямованість дії порушення на: конфіденційність, цілісність, доступність, а також на спостережливість та керованість АС.

4. Випадкові загрози суб'єктивної природи, тобто ті, що здійснюються через неуважність, недбалість або незнання. Наприклад: дії, які викликають збої АС (її складових частин) або знищення апаратних, програмних, інформаційних ресурсів (техніки, ліній зв'язку, втрату даних, програм і т. ін.); випадкове ушкодження носіїв; запуск тестових або технологічних процесів, які можуть спричинити непоправні зміни; ненавмисне впровадження в програмне забезпечення комп'ютерних вірусів; недотримання вимог до організаційних заходів захисту, що діють в АС розпорядчих документів; будь-які дії, які можуть призвести до розкриття таємних відомостей,

5. документів; будь-які дії, які можуть призвести до розкриття таємних відомостей, атрибутів розмежування доступу, втрати атрибутів і т. ін.; наслідки некваліфікованого застосування засобів захисту.

6. Навмисні загрози:

5.1 – порушення фізичної цілісності АС: пошкодження окремих компонентів, пристроїв, обладнання, носіїв інформації;

5.2 – порушення систем життєзабезпечення (таких як електроживлення, охоронна сигналізація, вентиляція тощо) та режимів функціонування обладнання і програмного забезпечення АС. Це може містити:

– виведення з ладу цих систем, що може призвести до небезпеки або втрати функціональності;

– в себе тимчасові або постійні відмови, збої, помилки або неправильне виконання функцій обладнання та програмного забезпечення;

5.3 – віруси та підслуховувальні пристрої: впровадження і використання комп'ютерних вірусів; використання закладних (апаратних і програмних) і підслуховувальних пристроїв;

5.4 – перехоплення побічних електромагнітних випромінювань через використання засобів перехоплення побічних електромагнітних випромінювань і акусто-електричних перетворень інформаційних сигналів;

5.5 – соціальні методи: використання шантажу, підкупу персоналу, введення в оману тощо;

5.6 – крадіжки і несанкціоноване копіювання інформації.

7. Інші загрози: читання залишкової інформації з оперативної пам'яті; отримання атрибутів доступу, а пізніше їх використання для підлаштування під зареєстрованого користувача, неправомірне під'єднання до каналів зв'язку, перехоплення даних та аналіз трафіку, а також впровадження і використання забороненого політикою безпеки програмного забезпечення або несанкціоноване використання ПЗ для отримання доступу до критичної інформації (наприклад, аналізаторів безпеки мереж).

З огляду на основні етапи, в процесі створення моделі загроз важливу увагу треба надати навмисним загрозам, а також іншим, які не можуть бути вирішені через впровадження організаційних заходів. Сучасні підходи до класифікації такого типу загроз доцільно розглядати через призму таких методів, як MITRE ATT&CK та Cyber Kill Chain by Lockheed Martin.

4. Аналіз методик Cyber Kill Chain by Lockheed Martin та MITRE ATT&CK

Методики Cyber Kill Chain by Lockheed Martin та MITRE ATT&CK важливі для створення моделей загроз та можуть застосовуватись для визначення стратегій захисту, в т. ч. під час розроблення КСЗІ для БІСК. Одна з перших створених методик, яка застосовується досі, Cyber Kill Chain, тобто "ланцюг ураження цілі", була розроблена компанією Lockheed Martin. Вона дає можливість простежувати етапи кібератаки, виявляє вразливості та допомагає командам з безпеки зупиняти атаки на кожному етапі ланцюга. Описує сім високорівневих цілей або тактик, які зловмисники виконують під час атаки. Ця методика допомагає розуміти, як відбувається атака та які кроки можуть бути вжиті для її запобігання. Наприклад, вона може бути використана для пояснення менеджменту, як може відбутись атака і як її можна зупинити. MITRE ATT&CK (The Adversarial Tactics, Techniques, and Common Knowledge), методика розроблена MITRE Corporation, є матрицею тактик, технік та процедур, які використовують зловмисники. ATT&CK дає можливість глибоко аналізувати конкретні методи атак та виявляти слабкі місця в захисті. Ця модель допомагає визначити, які методи можуть бути використані для захисту від конкретних загроз.

4.1. Методика Cyber Kill Chain

Методика Cyber Kill Chain, розроблена компанією Lockheed Martin, є частиною моделі Intelligence Driven Defense для ідентифікації та запобігання кібервторгненням. Методика визначає дії зловмисника, які він має виконати, щоб досягти своєї мети [9, 10]. Переривання дій зловмисника на одному етапі зупиняє атаку. Підходи методики Cyber Kill Chain представлено в таблиці.

Етапи реалізації методики Cyber Kill Chain

Етап	Зловмисник	Захисник
1	2	3
Розвідка (визначення цілі)	Зловмисники перебувають на етапі планування їхньої операції. Вони проводять дослідження, щоб зрозуміти, які цілі їм можна досягти	Виявлення розвідки, коли вона відбувається, може бути дуже складним, але коли захисники виявляють розвідку – навіть значно пізніше – це може виявити наміри супротивників
Озброєння (підготовка до операції)	Зловмисники перебувають на етапі підготовки. Відбувається генерація шкідливого програмного	Захисники не можуть виявити наявність шкідливого програмного забезпечення, але

Продовження таблиці

1	2	3
	забезпечення через автоматизовані інструменти	можуть зробити висновок, аналізуючи артефакти зловмисного програмного забезпечення
Доставка (початок операції)	Зловмисне програмне забезпечення доставляється в ціль	Це найважливіша можливість для захисників блокувати операцію. Основний захід ефективності – частка спроб вторгнення, які заблоковано на етапі доставки
Експлуатація (отримання доступу)	Зловмисники мають використовувати вразливість, щоб отримати доступ. Фраза “нульовий день” стосується коду експлойта, використаного лише на цьому кроці	Традиційні заходи безпеки додають стійкості, але спеціальні можливості потрібні, щоб зупинити експлойти нульового дня на цьому етапі
Встановлення (закріплення)	Зазвичай зловмисники встановлюють постійний бекдор або імплантують у середовищі жертви, щоб зберегти доступ упродовж тривалого часу	Інструменти кінцевої точки для виявлення та реєстрації активності встановлення. Проаналізуйте фазу встановлення під час аналізу зловмисного програмного забезпечення, щоб створити нові засоби пом’якшення кінцевих точок
Керування (дистанційне керування)	Зловмисне програмне забезпечення відкриває канал, щоб зловмисник міг віддалено маніпулювати жертвою	Останній шанс захисника заблокувати операцію: блокуванням каналу доступу. Якщо супротивники не можуть віддавати команди, захисники можуть запобігти удару
Дії згідно з цілями атаки (досягнення мети)	Маючи доступ, зловмисники досягнуть мети місії, що буде далі, залежить від його цілі	Чим довше зловмисник має доступ, тим більший його вплив. Захисники мають виявити цю стадію якнайшвидше, використовуючи й аналізуючи стан системи

Як бачимо з табл. 1, Cyber Kill Chain by Lockheed Martin складається з семи етапів, на яких описуються потенції дії як зловмисників, так і захисників. Ця методика підходить швидше для створення моделі порушника, ніж моделі загроз.

4.2. Методика ATT&CK

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) від компанії MITRE – це доступна база знань про тактику та прийоми зловмисників, яка ґрунтується на реальних спостереженнях. Ця методика допомагає фахівцям із кібербезпеки розробляти моделі та методології загроз, а також виявляти, запобігати та реагувати на кібератаки. Структурно ця методологія складається з матриці, яка описує загальні тактики, методи та процедури, які використовують зловмисники в різних доменах, таких як корпоративні, хмарні, мобільні та промислові системи керування [11, 12].

Кожна тактика представляє мету, яку може мати супротивник, наприклад початковий доступ, виконання, або вплив. Кожна техніка описує, як зловмисник може досягти цієї мети, як-от фішинг, зловмисне програмне забезпечення, скидання облікових даних, шифрування даних або зупинка служби. Структура також надає інформацію про джерела даних, засоби пом'якшення, групи, програмне забезпечення та кампанії, пов'язані з кожною технікою. MITRE ATT&CK регулярно оновлюється новими даними та думками від спільноти спеціалістів з безпеки.

Enterprise Matrix у структурі MITRE ATT&CK – це всеосяжна база знань про тактику та методи, які зловмисники використовують для компрометації, наполегливості, ескалації, ухилення, викрадення та порушення корпоративних систем і мереж. Матриця охоплює різні платформи, такі як Windows, macOS, Linux, хмарні служби, мережеві пристрої та контейнери, і містить детальну інформацію про поведінку, інструменти та стратегії пом'якшення для кожного методу. Матриця впорядкована за етапами атаки, від початкового доступу до впливу, і може допомогти групам безпеки зрозуміти, як думають і працюють кіберзловмисники, а також як виявляти та запобігати їхнім атакам. Матриця ґрунтується на реальних спостереженнях загроз кібербезпеці та постійно оновлюється новими даними та ідеями. Матрицю можна переглянути в ATT&CK Navigator, веб-інструменті, який дає можливість користувачам досліджувати та налаштовувати матрицю відповідно до своїх потреб.

Матриця мобільних пристроїв у MITRE ATT&CK є основою для розуміння та класифікації різноманітних тактик, прийомів і процедур, які використовують зловмисники під час атак на мобільні пристрої. Mobile Matrix охоплює дві основні сфери: доступ до пристрою та мережеві ефекти. Доступ до пристрою стосується методів, які потребують фізичного або логічного доступу до пристрою, як-от фішинг, використання чи доступ до облікових даних. Ефекти на основі мережі стосуються методів, які можуть використовувати зловмисники без доступу до пристрою, наприклад розвідка мережі, маніпулювання переданими даними або відмова кінцевої точки в обслуговуванні. Матриця мобільних пристроїв містить інформацію для платформ Android та iOS, а також докладну інформацію про те, як працює кожен метод, як його виявити та як запобігти чи пом'якшити його.

Матриця industrial control systems (ICS) – це база знань про дії зловмисників, метою яких є порушення систем промислового контролю (ICS). Це частина структури MITRE ATT&CK, яка є набором ресурсів із відкритим кодом і керованих спільнотою ресурсів для аналізу кіберзагроз. Матриця ICS складається з 12 тактик і 81 техніки, які описують, як зловмисники можуть скомпрометувати, маніпулювати або пошкодити пристрої, мережі та процеси ICS. Тактика – це окремі кроки, які зловмисники можуть використати для досягнення своїх кінцевих цілей, таких як початковий доступ, виконання, наполегливість, ухилення тощо. До 12 тактик належать:

1. Початковий доступ (Initial Access) – містить дванадцять технік.
2. Виконання (Execution) – містить дев'ять технік.
3. Наполегливість (Persistence) – містить шість технік.
4. Підвищення привілеїв (Privilege Escalation) – містить дві техніки.
5. Ухилення (Evasion) – містить шість технік.
6. Відкриття (Discovery) – містить п'ять технік.
7. Бічний рух (Lateral Movement) – містить сім технік.
8. Збірник (Collection) – містить одинадцять технік.
9. Командування і контроль (Command and Control) – містить три техніки.
10. Реагування на блокування (Inhibit Response Function) – містить чотирнадцять технік.
11. Порушення керування (Impair Process Control) – містить п'ять технік.
12. Вплив (Impact) – містить дванадцять технік.

Техніки представляють різні способи досягнення тактичних цілей, наприклад використання загальнодоступних програм, зміна завдань контролера, підробка звітних повідомлень тощо.

Матрицю ICS можна використовувати для оцінки рівня ризику середовищ ICS, виявлення прогалин у засобах безпеки та розробки стратегій пом'якшення. Також її можна використовувати

для аналізу поведінки противника, зіставлення активності загроз із певними методами та обміну інформацією про загрози між зацікавленими сторонами ICS.

5. Результати дослідження

Внаслідок дослідження проведено порівняння двох підходів Cyber Kill Chain та MITRE ATT&CK, які описують етапи дій порушника під час його проникнення в систему. MITER ATT&CK є більш детальною та комплексною на відміну від Cyber Kill Chain, що дає змогу для створення моделі загроз, яка охоплює всі аспекти поведінки зловмисника під час побудови КСЗІ.

З огляду на процес моделювання загроз для БІСК та складність даних систем, було визначено методику MITRE ATT&CK як ефективнішу для її використання під час побудови КСЗІ для БІСК.

Висновки

Запропоновано використання КСЗІ для побудови захищених БІСК як різновиду автоматизованої системи, в якій впроваджено інтелектуальні механізми у блоках керування для прийняття рішення на виконання дій без участі оператора. Першочергові заходи під час створення КСЗІ потребують створення моделі загроз.

Після проведеного аналізу двох методик Cyber Kill Chain by Lockheed Martin та MITRE ATT&CK для моделювання загроз під час створення КСЗІ в БІСК рекомендовано застосовувати MITRE ATT&CK. Одна з головних переваг MITRE ATT&CK над Cyber Kill Chain від Lockheed Martin під час створення моделі загроз полягає в тому, що MITRE ATT&CK забезпечує більш детальне та повне уявлення про поведінку зловмисника, тоді як Cyber Kill Chain пропонує більш високорівневий і лінійний вигляд процесу атаки.

MITRE ATT&CK охоплює повний спектр тактик, прийомів і процедур, які використовують зловмисники, від розвідки та початкового доступу до удару, а також надає стратегії пом'якшення та методи виявлення для кожного прийому. Він також пов'язує кожну техніку з розвідкою та дослідженнями реальних загроз, що полегшує розуміння контексту та актуальності кожної техніки. Cyber Kill Chain, з другого боку, фокусується на етапах атаки з погляду зловмисника. Він розбиває атаку на сім послідовних фаз: розвідка, озброєння, доставка, експлуатація, встановлення, керування, а також досягнення цілі. Це допомагає спеціалістам з безпеки зрозуміти процес зловмисника та потенційно перервати ланцюжок на будь-якому етапі. Однак ця методика не надає багато деталей про конкретні методи, які використовують зловмисники на кожному етапі, а також не пояснює складного, повторюваного і паралельного характеру кібератак. Також є тенденція ігнорувати внутрішні загрози та дії після зламу, які є важливими аспектами моделювання загроз.

На відміну від методики Cyber Kill Chain, яка охоплює лише сім загальних кроків дій зловмисника, методика ATT&CK (ICS) охоплює 12 тактик, кожна з яких містить певну кількість технік, що робить цю методику ефективнішою за Cyber Kill Chain.

Список літератури

1. Інтелектуальні інформаційні системи: структура і застосування [Текст] : підручник / О. М. Величко, Т. Б. Гордієнко; Держ. ун-т телекомунікацій. Херсон : Олді плюс, 2021. 727 с.

2. Багаторівневий захист технологій функціонування інтелектуальних об'єктів / В. Б. Дудикевич, Г. В. Микитин, М. О. Галунець, Р. Б. Кутень, Д. В. Васильєв, Г. А. Бабенцов // Стан, досягнення та перспективи інформаційних систем і технологій : матеріали XXII Всеукр. наук.-техн. конф. молодих вчених, аспірантів та студентів, Одеса, 21–22 квіт. 2022 р. / Одес. нац. технол. ун-т ; орг. ком: Б. В. Єгоров (голова) та ін. Одеса : ОНТУ, 2022. С. 58–60. Available at: https://card-file.ontu.edu.ua/items/a34a6bd6-2f11-45b9-95b6-d781c0cc6341

3. НД ТЗІ 1.1-003-99 Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. Available at: https://tzi.ua/assets/files/1.1_003_99.pdf

4. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, затверджений наказом Департаменту

спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. Available at: https://tzi.com.ua/downloads/2.5-005%20-99.pdf

5. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. Available at: https://tzi.com.ua/downloads/1.1-002-99.pdf

6. Гвоздьов Р. Ю. Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах [Текст] / Р. Ю. Гвоздьов, Р. В. Олійников // Радіотехніка. 2020. № 203. С. 91–96.

7. Сальник В. В., Гуж О. А., Закусіло В. С., Сальник С. В., Бєляєв П. В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 4(70). С. 77–82. https://doi.org/10.30748/zhups.2021.70.11

8. *НД ТЗІ 1.4–001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 04.12.2000 р. № 53. Available at: https://tzi.com.ua/downloads/1.4-001-2000.pdf*

9. Gaining the advantage. Applying Cyber Kill Chain Methodology to Network Defens. [Electronic resource]. Resource Access Mode: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

10. Singh V. K., Govindarasu M. Cyber Kill Chain-Based Hybrid Intrusion Detection System for Smart Grid. In Wide Area Power Systems Stability, Protection, and Security; Springer: Cham, Switzerland, 2021, pp. 571–599. http://dx.doi.org/10.1007/978-3-030-54275-7_22

11. What is ATT&CK? [Electronic resource]. Resource Access Mode: https://attack.mitre.org/

12. Roy S., Panaousis E., Noakes C., Laszka A., Panda S. and Loukas G. (2023) SoK: The MITRE ATT&CK Framework in Research and Practice. https://doi.org/10.48550/arXiv.2304.07411

APPROACHES TO THREAT MODELING IN THE CREATION OF A COMPREHENSIVE INFORMATION SECURITY SYSTEM FOR A MULTI-LEVEL INTELLIGENT CONTROL SYSTEMS

T. Kret

Lviv Polytechnic National University,
Information Security Department

The problem of modeling threats in the creation of a comprehensive information security system in multi-level intelligent control systems is considered. Existing approaches to creating a threat model are described. It is proposed to consider a multi-level intelligent control system as a type of automated system, according to the classification of Ukrainian normative documentation. The process of creating threat models for automated systems is analyzed.

To select the optimal methodology for creating a model in multilevel intelligent control systems, three methodologies (frameworks) that can be used for threat modeling were investigated: MITRE ATT&CK, Cyber Kill Chain by Lockheed Martin.

Based on a comparative analysis, the application of the MITRE ATT&CK methodology is justified as the most effective method for threat modeling in multilevel intelligent control systems.

Keywords: threat model, comprehensive information security system, multilevel intelligent management system, MITRE ATT&CK, Cyber Kill Chain by Lockheed Martin, CISS, MIMS.