УДК 623.618.51

БАГАТОКОНТУРНІ СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Євсеєв С. П., Король О. Г.

Постійно кількість загроз безпеці об'єктів критичної інфраструктури, до яких належать і соціокіберфізичні системи призводить до зниження якості послуг безпеки та рівня захищеності елементів інфраструктури. Об'єктом дослідження є процес побудови комплексної системи захисту в соціокіберфізичних системах. Ситуація, що склалася, не в останню чергу обумовлена недосконалістю застосовуваних сьогодні механізмів забезпечення безпеки елементів об'єктів критичної інфраструктури, до яких належать і соціокіберфізичні системи. Технологічна складність виявлення нових невідомих загроз безпеці, а також витонченість у методах їх реалізації зумовлює нагальну необхідність кардинального перегляду чинних підходів до її забезпечення. Отже, ставати зрозуміло, що розробка нового підходу до забезпечення безпеки інформаційних ресурсів у соціокіберфізичних системах. У статті запропоновано новий підхід методологічних засад побудови багатоконтурних систем захисту інформації із внутрішнім та зовнішнім контурами на кожній із платформ соціокіберфізичних систем. Такий підхід формується на універсальному класифікаторі загроз, який враховує не технічний аспект загроз, а і їх комплексування з методами соціальної інженерії, їхньої синергії гібридності. Враховується соціополітичний вплив на реалізацію загроз, а також запропоновано практичні механізми забезпечення основних послуг безпеки на основі постквантових алгоритмів. У рамках запропонованого підходу у загальному вигляді формалізовано проблему підвищення рівня захищеності інформації та визначено подальші шляхи її вирішення.

Проведений аналіз загроз на соціокіберфізичні системи (об'єкти критичної інфраструктури) дає змогу сформувати методологічні засади побудови багатоконтурних систем захисту інформації. Одним з основних елементів таких систем пропонується використовувати постквантові алгоритми – крипто-кодові конструкції на різних завадових кодах з можливістю завдання шкоди. Пропоновані крипто-кодові конструкції Мак-Еліса на LDPC-кодах забезпечують оперативність та стійкість, забезпечують необхідний рівень основних послуг безпеки.

Запропонована методологія побудови багатоконтурних систем захисту забезпечує можливість отримання об'єктивної оцінки поточного стану захищеності в социокиберфизических системах. Пропонований програмний комплекс оцінки дозволяє отримати інтегрований показник безпеки, виявити критичні точки вразливості та "можливість" зловмисника отримати доступ до конфіденційної інформації. А запропоновані механізми та протоколи на основі постквантових алгоритмів забезпечать необхідний рівень стійкості та оперативності у період появи повномасштабного квантового комп'ютера.

Ключові слова: соціокіберфізична система, безпека інформації, інформаційна безпека, кібербезпека, емерджентність..

***Ключові слова**: об'єкти критичної інфраструктури, безпека інформації, інформаційна безпека, кібербезпека, емерджентність.*

Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри, кафедра кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", вул. Кірпичова, 2, м. Харків, Україна, 61002
ORCID: https://orcid.org/0000-0003-1647-6444

Король Ольга Григорівна, кандидат технічних наук, доцент, кафедра кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", вул. Кірпичова, 2, м. Харків, Україна, 61002
ORCID: https://orcid.org/0000-0002-8733-9984