Гуменюк І. В., канд. техн. наук,
доцент кафедри захисту інформації та кібербезпеки,
Басараба М. С., курсант 271 навчальної групи,
Некрилов О. В., курсант 271 навчальної групи
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА ЗАХИСТУ ІНФОРМАЦІЇ ВАЖЛИВИХ КОМПОНЕНТІВ МЕРЕЖІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Кібернетичний простір завжди викликав великий інтерес у кіберзлочинної спільноти. За останніх п'ять років кібератаки здійснювалися на держустанови, сферу науки (освіти), фінансову, промислову та військову галузі. Прикладом тому є значна кількість атак, які сталися в світі: кібератака типу «credential stuffing» (початок 2019 року, Америка та Японія); кібератака типу «blackout» (березень 2019 року, Венесуела) тощо. В Україні в умовах складної та недостатньо стабільної політико-економічної ситуації такі випадки також мають місце. Наприклад, кібератака на інфраструктурні об'єкти держави (грудень 2015 року, Прикарпаття, Київська, Чернівецька області); кібератака на внутрішні телекомунікаційні мережі (грудень 2016 року, Міністерство фінансування України); масштабна кібернетична атака російських хакерів (червень 2018 року); понад 10 тисяч різних видів кібератак виявлено та заблоковано (травень – червень 2020 року).

Таким чином, в умовах, що склалися, актуальним є завдання розроблення нових дієвих, ефективних та удосконалення існуючих методів протидії кібернетичним атак та несанкціонованого доступу (НСД). Виходячи з даних передумов, сформульовано *мету даної роботи*, яка полягає у розробленні методики захисту важливих компонентів мережі інформаційно-телекомунікаційній системі (ІТС) для вирішення завдань своєчасного виявлення та протидії кібератак та НСД.

Забезпечення надійного та дієвого захисту інформації, важливих компонентів ІТС є комплексним завданням, яке включає в себе сукупність взаємопов'язаних між собою задач. Саме тому, для досягнення мети завдання запропоновано методику, яка складається з таких етапів:

1. Постійний контроль стану мережевих вузлів та каналів зв'язку мережі ІТС;
2. Фіксування фактів здійснення кібернетичних атак з детальним описом рівня небезпеки загроз;
3. Постійний контроль доступу користувачів до мереж ІТС;
4. Своєчасне виявлення НСД до мереж ІТС та оперативна протидія цим спробам та кіберзагрозам.

Детально розглянемо кожен із етапів.

Постійний контроль стану мережевих вузлів та каналів зв'язку мережі ІТС. Оскільки важливим завданням управління мереж є підтримання функціональності та надійності кожного мережевого компоненту, для ІТС необхідно використовувати ієрархічне управління, розподіливши мережу на окремі зони (кластери) з виділенням контролерів кластера, вузлів-шлюзів і внутрішніх вузлів кластера. В умовах успішного проведення кібератаки на вузли такий підхід ефективний для забезпечення фізичної ізоляції одного (потенційно-небезпечного) кластера з метою кіберзахисту іншого.

Фіксування фактів здійснення кібернетичних атак з детальним описом рівня небезпеки загроз можна здійснювати за допомогою систем виявлення вторгнень – Intrusion Detection System (IDS). На сучасному етапі розвитку інформаційних технологій такі системи є невід'ємною складовою забезпечення кібербезпеки будь-якої ІТС.

IDS, як правило, є програмою або апаратним засобом, який аналізує параметри вхідного та вихідного трафіку з метою виявлення фактів здійснення кібернетичних атак. При цьому, необхідно враховувати, що системи IDS – один з інструментів забезпечення кібербезпеки ІТС та не повинен розглядатися як заміна для будь-якого з інших захисних механізмів.

Постійний контроль доступу користувачів до мереж ІТС. Для забезпечення перевірки автентичності користувачів мережі ІТС на даному етапі здійснюється:

- виявлення та локалізація геометрії їх обличчя на зображені відеопотоку;
- обчислення набору базових ознак (характеристик) зображення;
- порівняння їх з еталонними, які містяться у базі даних.

Особливість біометричної автентифікації полягає у можливості її реалізації у мобільних додатках, що особливо актуально в умовах ін-форматизації сьогодення.

Своєчасне виявлення НСД до мереж ІТС та оперативна протидія цим спробам та кіберзагрозам виконується за умови скоєння кібератак та/або НСД. Виконання останнього етапу методики ґрунтується на узагальненні інформації про скоєння кіберзагрози або НСД, зокрема: власне сам факт здійснення кібернетичних атак (час, «компонент-жертва», нова або пов-торна загроза тощо); деталізований опис рівня небезпеки загрози.

Таким чином, у даній роботі наведено результати вирішення актуального науково-практичного завдання, яке полягало у розробленні методики захисту важливих компонентів мережі ІТС. Застосування методики дозволяє забезпечити своєчасне виявлення та підвищення протидії кібернетичним атакам та НСД до інформації, яка циркулює в ІТС.