Лобанчикова Н. М., канд., техн. наук, доцент,
доцент кафедри КІтаКБ,
Лобанчикова В. С., студентка, гр.ЗКБ-17
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЇ EDGE COMPUTING ПРИ ПОБУДОВІ IoT СИСТЕМИ ОХОРОНИ ПЕРИМЕТРУ

Розвиток інформаційних технологій та входження людства в четвер-ту промислову революцію (INDUSTRY 4.0), призвело до виникнення ряду новітніх технологій, що стрімко входять у наше життя, зокрема технології Інтернету речей (IoT). Їх впровадження з кожним роком зростає величезними темпами. IoT-системи впроваджуються, як у побуті, так і у промисловості, в цілому у діяльності людини. Не обійшло впровадження такого роду систем і об'єктів критичної інфраструктури. Все це створило нові загрози кібербезпеки у житті людства, нові виклики та можливості. Наслідки вдалих кібератак можуть бути катастрофічними, як для окремого члена суспільства, так і для нації, людства в цілому.

Дослідження процесів захисту від кібератак в інформаційному суспільстві набирає обертів та розділяється в залежності від об'єктів захисту. Задача мінімізації кібернетичних впливів внаслідок атак на IoT-системи є актуальною задачею сьогодення. Найбільша кількість атак припадає на портативні (кінцеві) пристрої, використання безпровідних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему. Особливо актуально дана задача ставиться при створенні систем охорони периметру військових об'єктів, об'єктів критичної інфраструктури та інших об'єктів, де реалізація атаки може мати геополітичне значення.

Підходи до побудови IoT постійно удосконалюються, так само як і технології, методи та підходи до їх захисту. Поява технологій edge computing направлена на вирішення кола задач кібербезпеки, концепція якої базується на децентралізованому зборі та обробці даних, тобто найближче до кінцевих IoT-пристроїв. Використання такого підходу при побудові IoT-систем має ряд переваг, зокрема:

- мінімізація часу на обробку та прийняття рішення;
- зменшення навантаження на канали передачі даних;
- зменшення об'ємів даних, що зберігаються в хмарі чи на фізичних серверах;
- зменшення навантаження на центри обробки даних (ЦОД).

Комбінування IoT та edge computing в сфері кібербезпеки може використовуватися для:

- моніторингу безпеки мережі;
- аутентифікації;
- шифрування;
- виявлення порушника в системах охорони периметру та контролю доступу;
- інформаційних відеосистемах при аналізі потоку даних та розпізнавання;
- аналітики безпеки у питаннях виявлення злоякісного програмного забезпечення, компрометації IoT-пристроїв та їх захопленні;
- прогнозування загроз;
- захисту інтерфейсу,
- механізмів доставки.

Провідну роль у кібербезпеці IoT відіграє компанія Cisco, що розробила і запропонувала ряд концептуальних і технічних рішень щодо захисту та дослідження IoT-технологій, в тому числі і IoT- систем. Зокрема розроблено фреймворк безпеки IoT, що став корисним доповненням до еталонної моделі.

Набір датчиків, що використовується в системах охорони периметру є визначеним, однак на кожному об'єкті різниться їх комбінування, розміщення, налаштування. Типовими є датчик руху, камера відеоспостереження, перепустка та сирена. Їх кількість буде залежати від периметру зони охорони, однак вони є типовими для більшості систем охорони. Для дослідження процесів кібернападів, проведемо моделювання кластеру системи охорони в програмному середовищі Cisco Packet Tracer, що включає відеокамеру, датчик руху, сирену, RFID-зчитувач та RFID-картку, шлюз для прийому/передачі інформації та відповідно монітор IoT. Ці пристрої і є стандартними компонентами IoT-системи охорони периметру. В залежності від території об'єкту охорони визначається необхідна кількість кластерів. Також на визначення кількості елементів системи впливають технічні характеристики вибраних засобів. Проведено підключення всіх IoT пристроїв та налаштування роботи системи, а також перевірено їх працездатність. Такого роду кластер використовуємо для моделювання та аналізу кібератак на такого роду системи, дослідження процесів відновлення системи після атак.

Така емуляція дозволяє розробити ряд практичних засобів щодо підвищення рівня кібербезпеки IoT-систем охорони периметру та безпосереднього впровадження на об'єктах захисту. Побудова комп'ютерна модель дозволяє нам визначити потенційні кіберзагрози та розробити технологію забезпечення кібербезпеки компонентів IoT.