КІБЕРБЕЗПЕКА СИСТЕМИ ОПОВІЩЕННЯ ТА ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ

Курепін В.М.
Миколаївський національний аграрний університет
kypins@ukr.net

Спроби порушити доступність, цілісність систем оповіщення та управління інформуванням населення під час воєнного стану в Україні відбуваються із завидною сталістю. Зловмисники перевантажують сервери системи управління інформуванням великою кількістю запитів, із-за чого мобільний приклад або центр управління оповіщенням може тимчасово припинити роботу, тимчасово не передати сигнал тривоги вчасно.

Найпоширенішим видом кіберзагрози є DDoS-атаки, які особливо критичні під час надзвичайних ситуацій. Вони здатні затримати сигнал повідомлення на кілька хвилин. Подібні випадки можуть вплинути на безпеку людей. Суттєві загрози слід чекати від підміни чи спотворення інформації. Злодії через несанкціонований доступ до каналів передачі даних надіслають хибні повідомлення про відбій тривоги або, навпаки. Це може спричинити паніку фальшивими сигналами про небезпеку. У практиці кіберінцидентів відомі випадки, коли через компрометацію регіональної системи оповіщення розповсюджувалися неправдиві SMS-повідомлення, що призводило до масового переміщення людей без реальної загрози.

Актуальними є загрози зараження шкідливими програмними забезпеченнями. Наприклад, програмами-вимагачами можуть заблокувати доступ до серверів управління оповіщенням та вимагати відновлення системи за викуп. Окремо слід враховувати ризики радіоелектронного та мережевого глушіння, коли порушується передача сигналів між компонентами системи, що знижує її оперативність та надійність.

Потенційно уразливими автоматизовані системи оповіщення населення роблять канали та вектори несанкціонованого втручання. Вони охоплюють як мережеву інфраструктуру, так і людський фактор.

Найпоширенішим каналом є віддалений доступ через мережу Інтернет. Зловмисники проникають до серверів управління через незахищені або неправильно налаштовані служби - відкриті порти, застаріле програмне забезпечення чи відсутність двофакторної автентифікації. У практиці відомі випадки, коли доступ до панелей управління системами оповіщення отримували через вразливість веб-інтерфейсів, що дозволяло змінювати налаштування або запускати несанкціоновані сигнали.

Фішингові атаки на персонал є іншим важливим вектором кіберзагрози. Населення отримує електронні листи або повідомлення, що імітують комунікацію, і, відкриваючи вкладення чи вводячи свої облікові дані, фактично передають доступ до злодіїв. Окремо слід відзначити фізичний доступ до обладнання, наприклад, до вузлів керування сиренами або мережевих шаф, коли сторонні особи можуть підключити шкідливі пристрої або змінити конфігурацію системи.

Не менш важливим каналом є внутрішні загрози - дії працівників, які мають легітимний доступ до системи. Вони можуть зловживати ним або ненавмисно створювати вразливості.

Наприклад, використовувати прості паролі або передають доступ третім особам. У сучасних умовах актуальними є атаки на ланцюги постачання програмного забезпечення. Шкідливий код вбудовується ще на етапі оновлення або встановлення системи, що дозволяє отримати скрытий контроль за її функціонуванням.

Отже, несанкціоноване втручання може здійснюватися комплексно, використовуючи одночасно технічні, організаційні та соціальні вектори впливу.