Пулеко І. В., к.т.н., доцент,
Свінцицька О. М., к.е.н, доцент,
Державний університет «Житомирська політехніка»
Чумакевич В. О., к.т.н., доцент,
Національний університет «Львівська політехніка»

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ «РОЗУМНОГО» БУДИНКУ

Для управління «розумними» будинками надзвичайно критичною є вимога інформаційної безпеки, адже успішні атаки означатимуть контроль зловмисника над приладами всередині будинку користувача, що є надзвичайно небезпечним та вкрай небажаним.

Загрозами інформаційної безпеки «розумного будинку» є порушення конфіденційності, цілісності та доступності інформації.

Загрози конфіденційності включають потенційні дії, які можуть призвести до неправомірного доступу до охоронюваних даних. Наприклад, порушення конфіденційності в системах «розумного» будинку може призвести до розкриття конфіденційних даних, таких як медичні. Навіть дані про внутрішню температуру будинку можуть бути використані для визначення його зайнятості. Втрата конфіденційності ключів та паролів може призвести до несанкціонованого доступу до системи. Загрози доступу є найбільш серйозними. Несанкціонований доступ до системного контролеру, особливо як адміністратора, робить всю систему небезпечною. Навіть якщо контроль не може бути отриманий, несанкціоноване підключення до мережі може викрасти пропускну здатність мережі або призвести до відмови в обслуговуванні законним користувачам. Багато пристроїв «розумного» будинку працюють від акумуляторної батареї і мають бездротову мережу з низьким робочим циклом, тому переповнення мережі запитами може призвести до атаки з виснаженням енергії – формі відмови в обслуговуванні.

До загроз доступу відноситься і слабка аутентифікація. Паролі є однією з перших ліній захисту від спроб злому. Але якщо ваш пароль недостатньо надійний, то і пристрій недостатньо захищений. Більшість паролів за замовчуванням є відносно слабкими, оскільки вони призначені для зміни, а в деяких випадках вони можуть бути загальнодоступними або зберігатися у вихідному коді програми.

Суттєвою вразливістю є доступність мережевої системи. Оскільки сучасні системи «розумний» будинок підключені до Інтернету, атаки можуть проводитися дистанційно, або за допомогою прямого доступу до мережевих інтерфейсів управління, або шляхом завантаження шкідливих програм на пристрої.

Фізична доступність системи також є проблемою. Як для бездротових технологій, так і для операторів зв'язку по лініях електропередачі, до фізичних мереж можна отримати доступ зовні, навіть якщо сам будинок надійно заблокований.

Наступна вразливість – обмежені системні ресурси. Контролери пристроїв часто мають обмежені обчислювальні та зберігальні ресурси, що ускладнює їх здатність до реалізації складних алгоритмів безпеки. Більшість додатків «розумного» будинку працюють з малою кількістю даних, що знижує витрати та продовжує термін служби батареї. Однак це ускладнює оновлення по повітрю і обмежує можливості використання функцій кібербезпеки, таких як брандмауери, антивірусні сканери та наскрізне шифрування.

Фіксована прошивка − ще одна проблема. Існує дуже мало розумних побутових приладів, які надають будь-які регулярні послуги з оновлення програмного забезпечення для виправлення вразливостей.

Системна неоднорідність також є вразливістю. Пристрої поставляються виробниками з різними мережевими стандартами і різними можливостями оновлення програмного забезпечення.

Застарілі пристрої в системі. Наприклад, старі пристрої можуть бути несумісними з новішими стандартами шифрування.

Повільне впровадження стандартів – це також вразливість. Немає універсального стандарту для всієї галузі, а це означає, що всі компанії та інші виробники повинні розробляти власні протоколи та рекомендації. Відсутність стандартизації ускладнює захист пристроїв Інтернету речей, а також ускладнює можливість міжмашинного зв’язку (M2M) без збільшення ризику.

Відсутність шифрування. Багато пристроїв (особливо старих) не шифрують дані, які вони надсилають, а це означає, що якщо хтось проникає в мережу, вони можуть перехопити облікові дані та іншу важливу інформацію, що передається на пристрій і з нього.

Суттєвою вразливістю є брак професійних спеціалістів з безпеки, які можуть керувати всіма складовими мережі «розумний» будинок.

Проблема виявлення атак та вторгнень є однією із найскладніших в інформаційній безпеці «розумного» будинку та потребує вирішення.