УДК 621.382 (045)

Третяк І.В., Маруш О.С., Пробита Д.М., Одарченко Р.С.
Національний авіаційний університет

Проблеми захисту інформації в концепції Smart University

Сучасний світ рухається у напрямі Smart технологій. Smart - це властивість об'єкта, що характеризує інтеграцію в даному об'єкті двох або більше елементів, які раніше не з'єднувались, і здійснюється з використанням Інтернет.[1]

На сьогоднішній день у життя втілюють у життя Smart будинки, офіси і навіть цілі міста, проте, поза увагою залишились навчальні заклади, що мають підвищувати адаптованість людини до життя. Інженер не працюючий у Smart середовищі не може повноцінно отримувати навички і працювати на благо технічного розвитку, дізнаючись про концепцію лише шляхом переглядання підручників, не досліджуючи процеси технічно та не маючи достатніх комфортних умов для здобування освіти. Smart концепції спрямовані не лише на покращення комфорту, вони значно поліпшують економічні проблеми. Тому ми пропонуємо нову концепцію, що має назву Smart University.

Smart University розглядається, як рішучий крок у майбутнє, унаслідок вдалих технологічних та архітектурних рішень. Це університет, у якому сукупність використання підготовленими людьми технологічних інновацій та Інтернету призводить до нового, відповідного смарт суспільству, якості процесів і результатів освітньої, науково-дослідної, комерційної, соціальної та іншої всебічної діяльності університету.

Заклад, у підґрунті якого закладені новітні технології, призначений для якісного, ефективного та комфортного освітнього процесу, як для студентів так і для працівників університету. Важливість технічного оснащення важко недооцінити у порівнянні з архітектурними рішеннями. Проте, архітектура та дизайн значно впливають з точки зору сприйняття студентами та науковцями такої організації, як університет. Найдоцільнішим з даної точки зору буде використання стилю хай тек, що вдало поєднується з технічним оснащенням університету майбутнього.

Smart University має:

Здійснювати контроль електроенергії та її доцільне використання;

Контроль освітлення приміщення;

Здійснювати контроль опалення приміщень та автономне регулювання;

Мати досконалу систему охорони, здійснюючи облік та контроль допуску осіб у навчальні приміщення кампусів та на територію університету;

Виконувати логічне об'єднання мережі різних підрозділів університету;

Інформування студентів та науковців актуальною інформацією через табло або пуш повідомлення;

Використання новітніх концепцій у роботі з обладнанням.

Більшу частину даних задач можна вирішити, використовуючи Internet of Things (далі – IoT). Так пункти у яких передбачений контроль фізичних параметрів можуть бути побудовані за рахунок використання сенсорних датчиків та безпровідної технології передачі даних.

IoT — концепція простору, в якій все з аналогового і цифрового світів може бути поєднане – це перевизначить наші відносини з об'єктами, а також властивості і суть самих об'єктів [2]. Інтернет речей –

це така концепція, що прагне за допомогою протоколів зв'язку та приладів з відповідним програмним забезпеченням здійснювати взаємодію між навколишнім середовищем і комп'ютерними системами та комп'ютерними системами між собою відповідно, при цьому, управління об'єктами може виконуватись віддалено.

Інтернет речей також став привабливим вектором здійснення DDoS-атак. Згідно зі звітом компанії InfoSec Institute, більшість «розумних» пристроїв для дому та малого бізнесу майже не захищені від атак зловмисників. У багатьох пристроях Інтернету речей містяться серйозні уразливості, а настройки безпеки за замовчуванням не витримують ніякої критики. Використовуючи відсутність повноцінних засобів моніторингу IPv6-трафіку, слабкий рівень захисту IPv4 / IPv6-шлюзів і величезну кількість незахищених пристроїв Інтернету речей, зловмисники зможуть створювати DDoS-ботнети величезних масштабів.

Розвиток концепції залежить від розвитку двох технологій – це радіочастотна ідентифікація (RFID) і бездротові сенсорні мережі (БСС).

Internet of Things має тісний зв'язок з поколінням смарт споруд та міст. Це пояснюється тим, що для цілісного функціонування складної системи будинку чи лікарні, наприклад, потрібне централізоване управління підсистемами, яке виконуватиме агент, що є об'єктом інтелектуальним у такій мірі, щоб мати змогу якісно виконати побажання власника на рівні цифрового світу, який матиме можливість впливати на роботу менш інтелектуальних агентів. Бездротову передачу даних виконуватимуть Mesh мережі, тобто такі мережі, де кожен вузол має рівноправні повноваження відносно інших. Розглянемо Wi-Fi, Zigbee і Bluetooth.

	ZigBee	Wi-Fi	Bluetooth
Діапазон	10-100 м	50-100 м	10 - 100 м
Топологія	Ad-Hoc, peer to peer, зірка,сітка	Точка-доступу	Ad-Hoc, дуже малі мережі
Робочая частота	868 МГц (Європа) 900-928 МГц (NA), 2,4 ГГц	2,4 і 5 ГГц	2,4 ГГц
Складність (пристроїв і додатків впливу)	Низький	Високий	Високий
Споживана потужність	Низький	Високий	Середа
Типові області застосування	Промислового контролю і моніторингу, сенсорних мереж, автоматизації будівель, управління і автоматизації будинку	Дозволяє розповсюджувати інформацію локальних мереж (LAN) до клієнтських пристроїв без проводів	Бездротове з'єднання між пристроями, такими як телефони, КПК, ноутбуки, навушники

Окреме місце серед розглянутих технологій відводиться сенсорним мережам. Сенсорна мережа – це безліч маленьких зчитувальних пристроїв (датчиків), здатних реєструвати зміни різних параметрів навколишнього середовища і транслювати ці

параметри іншим подібним пристроям, що знаходяться в зоні досяжності з певною метою.

Основними цілями використання сенсорних мереж можна назвати :

Системи безпеки;

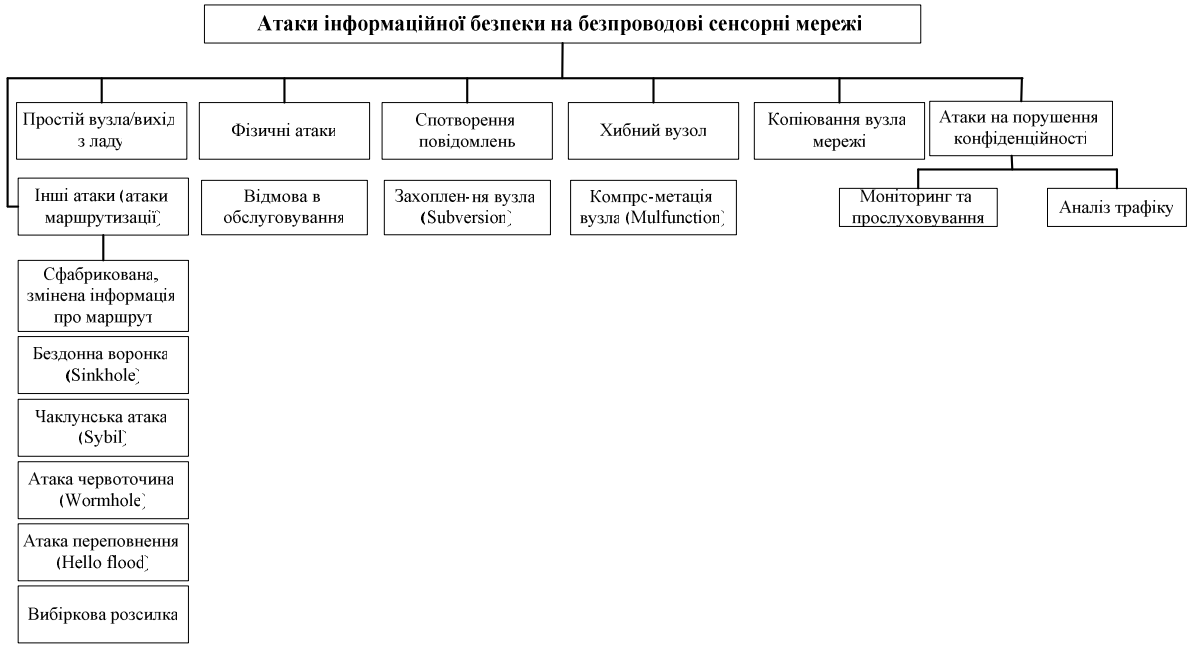
Системи моніторингу і контролю навколишнього;

Системи електроенергії;

Надзвичайні ситуації.

Нам знайомі основні цілі забезпечення інформаційної безпеки в БСМ: забезпечення конфіденційності, цілісності, аутентифікації і доступності даних, свіжість даних, самоорганізація, часова синхронізація, захищена локалізація.

Відомо, що бездротові мережі важко захистити внаслідок використання відкритого середовища в якості носія даних і широкомовної природи бездротових з'єднань. Саме тому існує багато мережевих атак в БСМ, класифікація яких приведена нижче [3] :



Для захисту сенсорних мереж використовують такі засоби:

Шифрування даних.

Різні рівні аутентифікації користувачів.

Захист від XSS-атак.

Фільтрація користувачів по IP і MAC-адресами.

Політики безпеки.

Висновки. В результаті проведеного дослідження було розглянуто нову концепцію Smart University. Очевидним є те, що дана концепція зробить наше життя простіше, але слід звернути увагу на використання безпровідних технологій, так як они є чутливими до певних видів атак, що може призводити до катастрофічних наслідків, були запропоновані основні ефективні механізми для захисту безпровідних мереж.

Список використаних джерел

1. *http://ojs.ifmo.ru*
2. *http://kyiv.comments.ua*
3. *Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах.*