УДК 007:004.56:351.824.11(824.11(477) DOI 10.33042/2522-1809-2020-4-157-184-191

В.Д. Бойко, М.Д. Василенко

Національний університет «Одеська юридична академія», Україна

"РОЗУМНЕ МІСТО" В КОНТЕКСТІ КІБЕРБЕЗПЕКИ: ІНЦИДЕНТИ, РИЗИКИ, ЗАГРОЗИ

У статті розкриваються джерела зовнішніх загроз і ефективні та неефективні методи захисту інформаційної екосистеми "розумного міста" ("air gap", пропрієтарні протоколи, "secure by obscure"). Наводяться приклади атак на інформаційні системи. Доведена недостатність відповідності системи «розумного міста» безпеко-захисним вимогам. Пропонується комплекс вимог і заходів до технічної сторони захисту інформаційно-комунікаційної інфраструктури "розумного міста".

Ключові слова: *розумне місто, інформаційні екосистеми, кібербезпека, муніципальне господарство, ризики, загрози, інциденти, захист.*

Постановка проблеми

Наразі накопичилася досить серйозна база знань з інцидентів і вразливостей в контексті "розумних міст". Найчастіше при аналізі інцидентів промислової та міської інфраструктури посилаються на аналіз поширення і збитку нанесеного Stuxnet [1] - мережевого хробака, націленого на руйнування центрифуг фірми Siemence, залучених в ядерній програмі Ірану.

Цей хробак поширювався мережею, використовуючи зараження флеш-накопичувачів і чотири уразливості категорії zero-day. Наприклад, зараження машини проводилося не за допомогою традиційного запуску autorun.inf, яке відомо всім і досить легко відстежується, і блокується засобами операційної системи, а за допомогою LNK-уразливості, яку складно виявити й купірувати.

Поширення хробака відбувалося до тих пір, поки він не опинявся на машині, яку розпізнавав, яка потрібна йому (тобто SCADA-система Siemence, що має певну конфігурацію). Після цього відбувалося перехоплення управління і виконання руйнівних дій. Цікаво, що таким чином (приховано заражаючи флешки) хробак зміг дістатися до комп'ютерів ядерної програми, які не мали виходу в Інтернет і вважалися захищеними від зовнішніх атак.

Ще одним відомим прикладом цілеспрямованого шкідника, націленого на ураження об'єктів промислової інфраструктури є вірус Triton [2, 3] який був націлений на атаку "останньої межі оборони" - виведення з ладу приладових систем безпеки (SIS) Schneider Triconex.

Найбільш відомими прикладами атак в Україні можуть служити епідемії WannaCry, Petya, збої української енергосистеми у 2015 році, описані в [4] і в [5].

Про готовність комп'ютерної інфраструктури свідчить динаміка зараження під час епідемій Ransomware Petya і WannaCry [6], коли більше третини комп'ютерних мереж (включаючи банківські та державні) виявилися виведеними з ладу. Загальний стан справ з еволюцією атак на об'єкти інфраструктури детально розглянуто в [7] і [8].

На момент написання статті, новітньою загрозою визнаний ransomware шифрувальник Snake, виявлений компанією FireEye (див. [9]) і націлений на виборчу атаку промислових об'єктів, які використовують обладнання General Electric. Наприклад, програма-вимагач атакувала сервер GE Digital Proficy [10].

При цьому експерти FireEye стверджують, що настав новий період в поширенні ransomware-шифрувальників - якщо до цього моменту вони були націлені "в простір" - тобто заражали будь-який доступний користувальницький комп'ютер, то в разі Snake можна говорити про цілеспрямовану, таргетовану загрозу конкретним об'єктам інфраструктури.

Наприклад, в дослідженні [11] показано наскільки просто зламуються світлофори в системі вуличного руху. Аналогічні випадки розбираються в роботі [12].

Аналіз останніх досліджень та публікацій

Останнім часом отримали популярність концепції розвитку "розумного міста". Існує кілька різних визначень цього терміну (див. [13]). Така ситуація пояснюється тим, що сфера питань впровадження IT-технологій у практику урбаністики є порівняно молодою навіть за мірками IT-індустрії. Сам по собі термін "розумне місто" має кілька різних визначень і перетинається з близькими за значенням термінами ("цифрове місто", "інтелектуальне місто" і так далі) -

детально еволюцію терміну можна простежити по роботі [14].

В якості точки відліку виникнення ідеї "розумних міст" зазвичай вказують книгу [15], в якій був використаний термін "розумне зростання" ("smart growth"). Пізніше, термін "розумне місто" ("smart city") був запропонований в роботі [16], який отримав подальший розвиток в [17]. Можна перерахувати ще кілька цікавих робіт по даному напрямку - це, наприклад роботи [18-20].

Теперішня концепція "розумного міста" бачиться як точка сходження декількох паралельних процесів, при якій інтеграція міських інформаційно-комунікаційних систем виходить на новий рівень. З таких тенденцій можна виділити наступні:

* насичення населення індивідуальними засобами комунікації (персональні комп'ютери, смартфони, планшети),

* розвиток загальноміських комунікаційних мереж (високошвидкісний мобільний інтернет),

* розвиток інтелектуальних систем управління виробництвом (АСУ ТП / ISC),

* розвиток "Інтернету речей" (IoT),

* поява інтегральних загальноміських мереж управління і спостереження за трафіком,

* поява "розумних квартир" і " розумних будинків".

Попри відмінність поглядів на розвиток міського середовища серед авторів, перерахованих вище, можна виділити кілька загальних моментів у розвитку і побудові " розумного міста":

* мережевоцентричний, розподілений підхід до формування міських інформаційних екосистем;

* ключове значення інформаційних технологій у розвитку міського середовища та його вплив на політичні та економічні міські системи;

* технології змінюють сприйняття, спосіб існування і сам міський ландшафт.

Більшість авторів сходиться на тому, що накопичення цифрових технологій призведе до переходу кількості в якість і в майбутньому можна буде говорити про "розумне місто", як про цілісну, єдину інформаційну екосистему (див. [19-21]), в якій Інформаційні технології відіграють ключову роль.

Така екосистема розумного міста може містити наступні елементи:

* система контролю дорожнього руху;

* система розподілу та управління стоянками;

* управління вуличним освітленням;

* управління громадським транспортом;

* управління постачанням води, енергії та вивезенням відходів;

* управління матеріальними ресурсами та логістикою;

* системи міської безпеки (камери, охоронні датчики й т. д.);

* системи загальноміського управління (в тому числі муніципальний документообіг);

* системи контролю навколишнього середовища;

* системи мобільного зв'язку;

* комунікаційні системи різного призначення.

Об'єднання всіх цих елементів дозволить в майбутньому створити максимально комфортну, безпечну і дружню до міського жителя середовище проживання. Наявність інтелектуальної складової сприятиме раціональному витрачанню ресурсів, а отже, дозволить використовувати енерго - і матеріалозберігаючі підходи і в цілому підвищити "ККД" міських ресурсів в цілому.

Впровадження концепції "розумного міста" при всіх перевагах, тягне за собою додаткові ризики і нові виклики для безпеки міської інфраструктури, а з нею і - політичного та економічного середовищ міста і в деяких випадках - ризики для життів жителів, які залежать від цих систем ([22]).

Мета статті полягає у здійсненні аналізу ризиків і загроз наявним і перспективним об'єктам "розумного міста", а також вироблення вимог і заходів до комплексної системи захисту, що дозволяє значною мірою копіювати загрози і знизити ризики для міської інформаційно-комунікаційної інфраструктури.

Виклад основного матеріалу дослідження

Основні джерела загроз і ризиків інформаційно-комунікаційної системи "розумного міста"

Можна виділити кілька джерел потенційних загроз і ризиків для міської інформаційно-комунікаційної інфраструктури, які існують вже зараз і будуть наростати в майбутньому.

Перш за все збільшуються "поверхні атаки" ("attack surface"). Глибока інтеграція міських інформаційно-комунікаційних систем - від смартфона рядового користувача до системи управління міським електротранспортом і АСУ ТП системи енергопостачання - потенційно збільшує "поверхню атаки" для зловмисників. Кожен доданий в систему елемент потенційно має свої власні уразливості, при цьому його інтеграція в загальний простір "розумного міста" означає, що зловмисник, використовуючи ці уразливості, може отримати з них доступ до загальноміської інфраструктури ([23]).

При цьому загальна складність системи призводить до того, що атака може породжувати різні види "ланцюгових реакцій", коли вихід з ладу одного сегмента (наприклад, управління міською енергосистемою) може вивести з ладу суміжні сегменти (наприклад, систему управління дорожнім рухом).

Крім збільшення "поверхні атаки", можна виділити наступні проблемні місця в безпеці сучасних

систем, покликаних обслуговувати інфраструктуру "розумного міста":

Нові технології часто впроваджуються і розгортаються без жодного тестування на безпечність. Розробники віддають перевагу простоті і легкості розгортання безпеки системи.

У більшості впроваджуваного апаратно-програмного забезпечення постійно знаходять уразливості. При цьому процес усунення сильно уповільнений і розтягнутий у часі в порівнянні з призначеним для користувача програмним забезпеченням — це особливо стосується пропрієтарного програмного забезпечення, підтримка якого здійснюється розробником без участі спільноти ("community"), а значить свідомо відстає від виявлення нових загроз.

Непропорційно великий сегмент технологій покладається на бездротові рішення. При цьому існує досить багато різних протоколів взаємодії, далеко не всі з яких відповідають стандартам безпеки. Така ситуація полегшує зловмиснику доступ до об'єкта атаки, відкриває додаткові уразливості в інформаційних системах, ще сильніше розширюючи поверхню атаки.

Відсутність єдиної міської служби кібербезпеки призводить до того, що інциденти в різних ділянках міської та суміжних інфраструктур, обробляються запізно і без загальної координації.

Технічна підтримка систем "розумного міста" утруднена і часто запізнюється. Як було зазначено вище розробники промислових та інфраструктурних інформаційних систем часто запізнюються з реакцією на нові загрози. Причини такої ситуації можна розділити на суб'єктивні і об'єктивні. До суб'єктивних, наприклад, може бути віднесений погляд розробників на міські та промислові системи, як на менш пріоритетні і другорядні в порівнянні з очевидними мішенями для атак, наприклад з фінансово-банківським сектором. Відповідно, на стадії розробки менше уваги і ресурсів приділяється забезпеченню безпеки і захисту від вторгнень.

До об'єктивних причин належать, наприклад, складнощі з експлуатацією вже впроваджених інформаційних систем, які забезпечують експлуатацію критичних ділянок інфраструктури. Зупинка або перебої в таких системах через невдале оновлення можуть спричинити значні збитки, якщо не матеріальні втрати. Тому, оновлення систем виконується рідко і з оглядкою на можливі наслідки.

Додатковим джерелом загроз є наявність в загальній системі ділянок, що обслуговуються застарілими системами з незакритими вразливостями. Заміна таких систем зазвичай відкладається до тих пір, поки не окупляться вкладення або поки в бюджеті не з'являться кошти. При цьому їх розробники можуть вже давно зняти системи з обслуговування - а це означає, що для виявлених в процесі експлуатації вразливостей і помилок не буде випущено оновлень. При цьому, завдяки загальній інтеграції систем "розумного міста", наявність в структурі "острівців архаїки" піддає ризику не тільки ці ділянки самі по собі, але і відкриває зловмиснику шлях до інших систем.

Чисто технічні джерела ризиків і загроз, доповнюються проблемами на організаційному рівні - відсутністю в міській структурі Єдиного центру реагування на кіберзагрози інфраструктурі, загальною бюрократизацією процесу, низькою кваліфікацією обслуговуючого персоналу, закритістю міських систем для спільноти розробників.

Вихід з ладу об'єктів інфраструктури може бути як результатом цілеспрямованої (таргетованої) атаки зловмисника (Stuxnet), так і побічним ефектом від загальної глобальної атаки на інформаційну систему. Прикладом останнього є епідемія WannaCry і Petya, які, поширившись по комп'ютерних мережах "зачепили" банківський сектор і енергетику.

Перераховані вище джерела загроз означають, що зломи таких систем - питання часу. При цьому додаткову небезпеку становить те, що з деякого моменту часу намітився тренд, при якому все більше зломів і атак інтелектуальних систем проводиться не з метою самоствердження зловмисника, а з метою заробітку грошей на наслідках зломів.

На ранній стадії основним об'єктом атак були фінансові та платіжні системи: підробка реквізитів банківських кредитних карт, злом кодувань супутникових телевізійних каналів і так далі.

На наступному етапі зломи стали інтелектуальніше - зокрема злом мережі банкоматів з метою отримання грошей і ransomware - шкідливі додатки, що шифрують диск і пропонують переказати гроші для дешифрування.

В даний час об'єктом атак стають об'єкти промислової та міської інфраструктури. На такі атаки з'явився попит, а це свідчить в найближчому майбутньому, що можна очікувати значне збільшення пропозиції (див. [20] і оцінку у [24]).

При цьому метою таргетованої атаки не обов'язково повинно бути виведення з ладу будь-якого об'єкта або керівної системи. Все більше атак робиться для отримання приватної і не підлягаючої розголошенню інформації (наприклад після атаки на Korea Hydro & Nuclear Power Co., Ltd. (KHNP), зловмисники отримали доступ до креслень та інструкцій для атомних реакторів [25]).

Перспективні системи захисту "розумного міста"

Перераховані вище випадки наочно демонструють необхідність комплексної системи забезпечення безпеки даних "розумного міста", яка б працювала на всіх рівнях інформаційної системи.

Вимоги до таких систем зазвичай пред'являються на трьох основних рівнях: законодавчому, організаційному та технічному. Законодавчі аспекти висвітлені в досить докладному огляді [26], а також в роботах [27] і [28].

Організаційні заходи перераховані в [29] і в [30] і можуть бути зведені до декількох рекомендацій - організації єдиних центрів реагування на загрозу, планування реакції на події і загрози різного рівня пріоритетності, пен-тестингу (тестування структури міських інформаційно-комунікаційних мереж на злом, проникнення, стійкість до шкідливих впливів), більш щільної взаємодії з розробниками програмного і апаратного забезпечення для міських інформаційних екосистем.

На наш погляд, слід приділяти більше уваги суто технічним вимогам до побудови та розвитку систем захисту "розумних міст". Це диктується тим, що інформаційна система "розумного міста" за своїм вихідним призначенням є відкритою системою - це означає, що як мінімум всі її бінарні компоненти зазвичай знаходяться в загальному доступі і доступні для дослідження потенційним зловмисникам.

1. Технічні вимоги до системи захисту "розумного міста"

На наш погляд, система захисту "розумного міста" повинна відповідати наступним вимогам:

* використовувати програмне забезпечення з відкритим вихідним кодом;

* використовувати відкриті протоколи обміну даними;

* використовувати відкриті стандарти зберігання даних;

* не покладатися на практику приховування даних, як на ефективну захисну міру;

* не покладатися на "повітряний просвіт", як на ефективну захисну міру;

* повинна легко масштабуватися;

* повинна мінімізувати труднощі з оновленням робочих компонентів;

* повинна передбачати;

* повинна дозволяти інтегрувати в себе майбутні ефективні рішення і розширення функціоналу;

* повинна бути децентралізованою або хоча б охоплювати елементи децентралізації;

* повинна дозволяти використання рівнів, ролей і прав доступу до даних;

Розглянемо перераховані вимоги докладніше.

2. Неефективні заходи захисту

Як було сказано вище, система "розумного міста" за своєю природою відкрита для будь-яких досліджень бінарних файлів, тому практика захисту даних шляхом приховування і умовчання ("secure by obscure") є неефективною-при достатній кількості часу і ресурсів аналіз бінарних файлів дозволить виявити будь-які спеціально залишені "бекдори" і "вразливі місця". Тому, захист такої системи не повинна покладатися на закритість вихідних кодів (хоча ніхто не забороняє використовувати це як додатковий рівень захисту - але слід розуміти всю ефемерність цього рівня).

Приклад атаки Stuxnet показує, що сучасне шкідливе програмне забезпечення досить легко долає "повітряний зазор" ("air gap"). Зокрема, поширеною практикою є USB Drop attack - коли зараження відбувається через флеш-накопичувачі, вільно або мимоволі підключаються до системи. Один з варіантів такого зараження навіть передбачає використання спеціального пристрою для атаки. Такий пристрій замасковано під звичайний флеш-накопичувач, проте всередині містить іншу апаратну начинку, яка спрацьовує при підключенні "помилкової флешки" в usb-порт. Таким чином, в сучасних реаліях навіть повне відключення від зовнішніх мереж зв'язку не гарантує безпеку. При цьому прагнення до створення air gap часто призводить до зниження загальної ефективності системи і підвищення витрат на її експлуатацію. Це особливо актуально для "розумного міста", де більшість систем розраховані на збір і обробку інформації в оперативному режимі і втрачають цінність для "офлайнових" контекстів. У цьому випадку організація "air gap" створює більше проблем, ніж вирішує.

3. Відкритість вихідних кодів для програмного забезпечення інформаційній екосистемі " розумного міста"

Вимога відкритості вихідних кодів, протоколів і стандартів обміну даними націлена на вирішення цілого спектру проблем, пов'язаного з пропрієтарним програмним забезпеченням і пропрієтарними протоколами і форматами зберігання даних.

У розробці програмного забезпечення давно склалася два напрямки розробки - відкритий, при якому клієнту поставляються в тому числі вихідні коди програмного забезпечення і закритий - коли клієнту поставляються тільки бінарні файли.

Аналогічним чином виглядає ситуація з відкритими і закритими форматами даних - в разі відкритого формату даних, специфікація на нього відома і доступна для використання іншим розробникам, в разі закритого формату даних специфікація відома тільки творцеві формату. У цьому випадку для сторонніх розробників немає можливості (або потрібні серйозні фінансові вкладення на покупку ліцензії) створювати додатки, що використовують даний формат. У таких ситуаціях сторонні розробники часто вдаються до використання реверс-інжинірингу ("reverse engineering") для самостійного аналізу і розкриття специфікацій формату, однак, цей шлях не завжди легальний і може переслідуватися за законом.

Пропрієтарні, закриті вихідні коди, протоколи взаємодії і формати даних виглядають досить логічним рішенням особливо у випадках, коли розробник бере

на себе поставку і розгортання системи "під ключ", а також забезпечує подальшу технічну підтримку, проте на практиці породжують цілий спектр проблем.

Перша з них - "vendor lock-in" - прагнення постачальників послуг замкнути клієнта на себе, монополізувавши надання послуги. Це відкриває розробнику можливість надалі вносити небажані і невигідні зміни в умови поставки послуги. Як правило, на цьому етапі в організацію і розгортання системи вже вкладені досить великі кошти, тому відхід від розробника стає невигідним, що змушує миритися з новими умовами.

Друга - можлива наявність "чорних ходів" ("backdoors"). Широко поширена практика, коли розробник залишає в системі "чорний хід" - свідомо ослаблене місце в системі, про який відомо тільки розробнику і яке розробник може використовувати для технічної підтримки за запитом клієнта - наприклад для відновлення втрачених клієнтом ключів для входу в систему або випадково видалених даних. Зазвичай офіційно декларується саме ця причина.

Однак, на практиці, в системах із закритим вихідним кодом наявність "бекдорів" залишається прихованим і їх експлуатація розробниками ніяк не може бути проконтрольована, що відкриває перед розробником широкі можливості для збору конфіденційної інформації та експлуатації системи в своїх інтересах.

Третя проблема полягає в тому, що "бекдор" відносно легко може бути виявлений при аналізі системи зловмисником - і використаний ним у своїх цілях. Багато зломів засновані саме на використанні свідомо закладених в систему розробником (самостійно або на вимогу клієнтів) вразливостей.

Також при використанні закритого програмного забезпечення, виникає ризик втрати можливості обслуговування системи в тому випадку, якщо її Розробник збанкрутує, піде з ринку або його компанія буде поглинена іншим розробником - такі ситуації трапляються досить часто (Див, наприклад [31] і [32]).

Так само, у випадку одного, монопольного постачальника послуг не виключений ризик потрапляння під санкції того чи іншого роду - характерним випадком є заборона корпорацією Google оновлень операційної системи на смартфонах корпорації Huawei ([33]).

4. Відкриті стандарти взаємодії в інформаційній екосистемі "розумного міста"

Відкриті стандарти взаємодії дозволяють так само розв'язати проблему децентралізації і стикування декількох систем або підсистем від різних виробників. Хорошим прикладом взаємодії в сучасному світі є телефонна мережа і мережа Інтернет, коли обладнання, вироблене різними розробниками і містять не тільки термінальні пристрої (телефони, планшети, ноутбуки і т.д.), але і серверні системи (телефонні станції, шлюзи, маршрутизатори і так далі) відразу доступні до підключення і роботі в загальній мережі передачі інформації. Складно обґрунтувати цінність телефонної станції, яка працює тільки з телефонами певних моделей і може пов'язувати абонентів тільки між собою, без виходу на зовнішні станції.

Міська система безпеки повинна передбачати масштабування - слід вже на стадії планування впровадження і розгортання системи загадуватися над питаннями стабільності продуктивності системи при зростанні її розмірів і підключенні додаткових систем.

Використання відкритих стандартів для "розумного міста" і для його систем безпеки не тільки полегшує загальну внутрішню організацію міських підсистем - "розумних будинків", підприємств, транспорту, міської інфраструктури та окремих пристроїв, але і потенційно робить можливим створення "розумних регіонів", "розумних країн" і так далі - за аналогією з наявними зараз телефонними та інформаційними мережами. На прикладі телефонних та інформаційних мереж можна показати, що збільшення розмірів і охоплення мережі підвищує як загальну цінність, так і цінність окремих її сегментів.

Перераховані вимоги можуть здатися досить жорсткими, але в принципі досяжні на поточному рівні розвитку інформаційних технологій. Існують і досить поширені відкриті системи і протоколи взаємодії.

При цьому основний шлях захисту даних у відкритих системах в даний час бачиться у використанні засобів асиметричної криптографії з відкритими ключами - можна послатися на класичний приклад PGP/GnuPG, однак зразковою реалізацією такої системи на наш погляд є специфікація шифрування носіїв LUKS, яка дає приклади хорошої організації захисту даних і зручного для користувача управління ключами.

5. Технології децентралізації інформаційної екосистеми "розумного міста"

При великих масштабах охоплення набуває значення децентралізація інформації в мережі оскільки цілісність навіть міської мережі не повинна залежати від справності окремого сервера або навіть системи серверів. В рамках проблеми безпеки "розумного міста" децентралізація набуває життєво важливого значення. Якщо зловмиснику вдасться зламати або вивести з ладу один з елементів системи (наприклад, виробничу систему), це не повинно автоматично приводити до виходу з ладу інших елементів - транспорту, зв'язку, енергопостачання.

Для децентралізації та підтримки цілісності даних перспективним є використання технології зв'язкових списків (блокчейнів). В даний час технології блокчейну відомі в основному як основа для організації криптовалютних систем і заробили цим незаслужено погану славу. Насправді блокчейни

надають набагато ширше поле для використання. Ця технологія якнайкраще підходить для управління захистом і забезпечення цілісності даних в розподілених системах. При цьому для "підпису" поширюваних в системі даних використовуються досить низькі за вимогами до обчислювальних ресурсів технології - що дозволяє використовувати блокчейн технології навіть в низькорівневих додатках і відносно скромних за технічними характеристиками апаратних системах.

Ще однією перевагою блокчейна є можливість зберігання, поширення і підтримки цілісності даних навіть якщо ці дані зберігаються у відкритій формі - в цьому випадку блокчейн працює як гарантія цілісності даних і захисту їх від модифікації третьою стороною "на льоту" (див. наприклад [34]).

Це дозволяє використовувати блокчейн не тільки для взаємодії систем в реальному часі, але і для зберігання та архівації важливих документальних даних системи.

Висновки

Таким чином, сучасні тренди вказують на висхідний інтерес зловмисників до зломів окремих підсистем "розумних міст", при цьому самі системи "розумного міста" ще недостатньо відповідають вимогам безпеки та захисту від зовнішніх загроз. Це вимагає при розробці, плануванні впровадженні та розгортанні "розумного міста" передбачати комплексну систему захисту, яка відповідала б вимогам відкритості, розширюваності та децентралізації й не покладалася б на застарілі та неефективні методи захисту ("air gap", пропрієтарні протоколи, "secure by obscure" і так далі). На наш погляд цим вимогам відповідає широке використання програмного забезпечення з відкритими вихідними кодами, що використовує відкриті стандарти зберігання, передачі й перетворення інформації та широко залучає сучасні криптографічні засоби (асиметричну криптографію з відкритими ключами) і засоби забезпечення цілісності та децентралізації зберігання даних (блокчейн). Все це дозволить значно підвищити стійкість, живучість й безпеку систем "розумного міста".

Література

1. Barzashka I. Are cyber-weapons effective? Assessing stuxnet's impact on the iranian enrichment programme // The RUSI Journal. — Taylor & Francis, 2013. — Vol. 158, no. 2. — P. 48–56.
2. Di Pinto A., Dragoni Y., Carcano A. TRITON: The first ics cyber attack on safety instrument systems / Proc. Black hat usa. — 2018. — P. 1–26.
3. Lee R. TRISIS malware: Analysis of safety system targeted malware. Dragos inc. — 2017. — https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
4. Case D. U. Analysis of the cyber attack on the Ukrainian power grid // Electricity Information Sharing and Analysis Center (E-ISAC). — 2016. — Vol. 388. — Available: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
5. Slowik J. CRASHOVERRIDE: Reassessing the 2016 Ukraine electric power event as a protection-focused attack // Dragos, Washington, DC, USA, Tech. Rep., Aug. — 2019. — https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
6. Fayi S. Y. A. What petya/notpetya ransomware is and what its remidiations are // Information technology-new generations. — Springer, 2018. — P. 93–100.
7. Slowik J. Evolution of ics attacks and the prospects for future disruptive events. — Accessed: Feb, 2020.
8. Branquinho M. A. Ransomware in industrial control systems. What comes after wannacry and petya global attacks? // WIT Transactions on The Built Environment. — WIT Press, 2018. — Vol. 174. — P. 329–334.
9. Ransomware Against the Machine: How Adversaries are Learning to Disrupt / FireEye. — 2020. — https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html
10. Financially Motivated Actors Are Expanding Access Into OT: Analysis of / FireEye. — 2020. — https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html#:~:text=Threat%20Research-,Financially%20Motivated%20Actors%20Are%20Expanding%20Access%20Into%20OT%3A%20Analysis%20of,Used%20With%20Seven%20Malware%20Families&text=For%20example%2C%20the%20shift%20to,adapt%20to%20more%20complex%20environments.
11. Ghena B., Beyer W., Hillaker A., Pevarnek J., Halderman J. A. Green lights forever: Analyzing the security of traffic infrastructure / 8th USENIX workshop on offensive technologies (WOOT 14). — San Diego, CA: USENIX Association, 2014. — https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf
12. Cerrudo C. Hacking traffic control systems (us, uk, australia, france, etc.) // DEF CON. — 2014. — Vol. 22. — P. 1-5.
13. Perätalo S., Ahokangas P. Toward smart city business models // Journal of Business Models. — 2018. — Vol. 6, no. 2. — P. 65–70.
14. Cocchia A. Smart and digital city: A systematic literature review // Smart city. — Springer, 2014. — P. 13–43.
15. Bollier D. How smart growth can stop sprawl: A fledgling citizen movement expands. — Essential Books, 1998. — 90 p.
16. Komninos N. The architecture of intelligent cities // Intelligent Environments. — IET, 2006. — Vol. 6. — P. 53–61.
17. Komninos N. Intelligent cities and globalisation of innovation networks. — Routledge, 2008. — file:///C:/Users/HP/Downloads/Intelligent-Cities-and-Globalisation-of-Innovation-Networks.pdf
18. Schuler D. Digital cities and digital citizens / Kyoto workshop on digital cities. — Springer, 2001. — P. 71–85.
19. Deren L., Zhenfeng S., Xiaomin Y. Theory and practice from digital city to smart city [j] // Geospatial Information. — 2011. — Vol. 6. — P. 002.
20. Zygiaris S. Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems // Journal of the knowledge economy. — Springer, 2013. — Vol. 4, no. 2. — P. 217–231.

21. Tokody D., Schuster G. Driving forces behind smart city implementations-the next smart revolution // Journal of Emerging research and solutions in ICT. — FICT, 2016. — Vol. 1, no. 2. — P. 1–16.
22. Braun T., Fung B. C., Iqbal F., Shah B. Security and privacy challenges in smart cities // Sustainable cities and society. — Elsevier, 2018. — Vol. 39. — P. 499–507.
23. Cerrudo C. Hacking smart cities / RSA conference. — 2015. — P. 2–18.
24. Friis K., Muller L. P., Gjesvik L. Cyber-weapons in international politics: Possible sabotage against the norwegian petroleum sector // NUPI Report. — NUPI, 2018. — https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1
25. Lee K.-b., Lim J.-i. The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the korea hydro & nuclear power co., ltd. // KSII Transactions on Internet & Information Systems. — 2016. — Vol. 10, no. 2. — P. 857-880.
26. Losavio M. M., Chow K. P., Koltay A., James J. The internet of things and the smart city: Legal challenges with digital forensics, privacy, and security // Security and Privacy. — 2018. — Vol. 1, no. 3. — P. e23.
27. Song H., Srinivasan R., Sookoor T., Jeschke S. Smart cities: Foundations, principles, and applications. — John Wiley & Sons, 2017. — 912 p.
28. Elmaghraby A. S., Losavio M. M. Cyber security challenges in smart cities: Safety, security and privacy // Journal of advanced research. — Elsevier, 2014. — Vol. 5, no. 4. — P. 491–497.
29. Lacinák M., Ristvej J. Smart city, safety and security // Procedia engineering. — Elsevier, 2017. — Vol. 192. — P. 522–527.
30. Rawat D. B., Ghafoor K. Z. Smart cities cybersecurity and privacy. — Elsevier, 2018. — 303 p.
31. Opara-Martins J., Sahandi R., Tian F. Critical review of vendor lock-in and its impact on adoption of cloud computing / International conference on information society (i-society 2014). — 2014. — P. 92–97.
32. Pellegrini R., Rottmann P., Strieder G. Preventing vendor lock-ins via an interoperable multi-cloud deployment approach / 2017 12th international conference for internet technology and secured transactions (icitst). — 2017. — P. 382–387.
33. Singh G. (2019). China-us trade war: An overview // Manag Econ Res J. — HATASO, 2019. — Vol. 5, no. 2019. — P. 10805.
34. Sun J., Yan J., Zhang K. Z. Blockchain-based sharing services: What blockchain technology can contribute to smart cities // Financial Innovation. — SpringerOpen, 2016. — Vol. 2, no. 1. — P. 1–9.

References

1. Barzashka I. (2013). Are cyber-weapons effective? Assessing stuxnet's impact on the iranian enrichment programme. *The RUSI Journal*, 158(2), 48–56.
2. Di Pinto A., Dragoni Y., Carcano A. (2018). TRITON: The first ics cyber attack on safety instrument systems / Proc. Black hat usa., 1–26.
3. Lee R. (2017). TRISIS malware: Analysis of safety system targeted malware. Dragos inc. Retrieved from https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
4. Case D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid // Electricity Information Sharing and Analysis Center (E-ISAC), 388. Retrieved from https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
5. Slowik J. (2019). CRASHOVERRIDE: Reassessing the 2016 Ukraine electric power event as a protection-focused attack. Dragos, Washington, DC, USA, Tech. Rep.. Retrieved from https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
6. Fayi S. Y. A. (2018). What petya/notpetya ransomware is and what its remidiations are. *Information technology-new generations*, 93–100.
7. Slowik J. (2020). Evolution of ics attacks and the prospects for future disruptive events. — Accessed: Feb, 2020.
8. Branquinho M. A. (2018). Ransomware in industrial control systems. What comes after wannacry and petya global attacks? // WIT Transactions on The Built Environment. — WIT Press, 174, 329–334.
9. Ransomware Against the Machine: How Adversaries are Learning to Disrupt / FireEye. — 2020. Retrieved from https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html
10. Financially Motivated Actors Are Expanding Access Into OT: Analysis of / FireEye. — 2020. Retrieved from https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html#:~:text=Threat%20Research-,Financially%20Motivated%20Actors%20Are%20Expanding%20Access%20Into%20OT%3A%20Analysis%20of,Used%20With%20Seven%20Malware%20Families&text=For%20example%2C%20the%20shift%20to,adapt%20to%20more%20complex%20environments.
11. Ghena B., Beyer W., Hillaker A., Pevarnek J., Halderman J. A. (2014). Green lights forever: Analyzing the security of traffic infrastructure / 8th USENIX workshop on offensive technologies (WOOT 14). — San Diego, CA: USENIX Association. Retrieved fromhttps://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf
12. Cerrudo C. (2014). Hacking traffic control systems (us, uk, australia, france, etc.). DEF CON, 22, 1-5.
13. Perätalo S., Ahokangas P. (2018). Toward smart city business models. *Journal of Business Models*, 6(2), 65–70.
14. Cocchia A. (2014). Smart and digital city: A systematic literature review. *Smart city*, 13–43.
15. Bollier D. (1998). How smart growth can stop sprawl: A fledgling citizen movement expands. Essential Books, 90.
16. Komninos N. (2006). The architecture of intelligent cities. *Intelligent Environments*. — IET, 6, 53–61.
17. Komninos N. (2008). Intelligent cities and globalisation of innovation networks. — Routledge. Retrieved from file:///C:/Users/HP/Downloads/Intelligent-Cities-and-Globalisation-of-Innovation-Networks.pdf
18. Schuler D. (2001). Digital cities and digital citizens. *Kyoto workshop on digital cities*, 71–85.
19. Deren L., Zhenfeng S., Xiaomin Y. (2011). Theory and practice from digital city to smart city [j]. *Geospatial Information*, 6, 002.
20. Zygiaris S. (2013). Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. *Journal of the knowledge economy*, 4(2), 217–231.
21. Tokody D., Schuster G. (2016). Driving forces behind smart city implementations-the next smart revolution. *Journal of Emerging research and solutions in ICT*, 1(2), 1–16.

22. Braun T., Fung B. C., Iqbal F., Shah B. (2018). Security and privacy challenges in smart cities. *Sustainable cities and society*, 39, 499–507.
23. Cerrudo C. (2015). Hacking smart cities. *RSA conference*, 2–18.
24. Friis K., Muller L. P., Gjesvik L. (2018). Cyber-weapons in international politics: Possible sabotage against the norwegian petroleum sector. *NUPI Report*. Retrieved from https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1
25. Lee K.-b., Lim J.-i. (2016). The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the korea hydro & nuclear power co., ltd. *KSII Transactions on Internet & Information Systems*, 10(2), 857-880.
26. Losavio M. M., Chow K. P., Koltay A., James J. (2018). The internet of things and the smart city: Legal challenges with digital forensics, privacy, and security. *Security and Privacy*. 1(3), e23.
27. Song H., Srinivasan R., Sookoor T., Jeschke S. (2017). Smart cities: Foundations, principles, and applications. John Wiley & Sons, 912.
28. Elmaghraby A. S., Losavio M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of advanced research*, 5(4), 491–497.
29. Lacinák M., Ristvej J. (2017). Smart city, safety and security. *Procedia engineering*, 192, 522–527.
30. Rawat D. B., Ghafoor K. Z. (2018). Smart cities cybersecurity and privacy. *Elsevier*, 303.
31. Opara-Martins J., Sahandi R., Tian F. (2014). Critical review of vendor lock-in and its impact on adoption of cloud computing. International conference on information society (i-society 2014), 92–97.
32. Pellegrini R., Rottmann P., Strieder G. (2017). Preventing vendor lock-ins via an interoperable multi-cloud deployment approach. 2017 12th international conference for internet technology and secured transactions (icitst), 382–387.
33. Singh G. (2019). China-us trade war: An overview. Manag Econ Res J. — HATASO, 5, 10805.
34. Sun J., Yan J., Zhang K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, 2(1), 1–9.

Рецензент: д-р техн. наук, проф. В.М. Тупкало, Інститут інтелектуальної власності та права Національного Університету "Одеська юридична академія", Київ, Україна.

Автор: БОЙКО Віктор Дмитрович
кандидат технічних наук, доцент кафедри кібербезпеки
Національний університет «Одеська юридична академія»
E-mail – boyko-work@ukr.net
ID ORCID:http://orcid.org/0000-0001-5929-657X

Автор: ВАСИЛЕНКО Микола Дмитрович
доктор фізико-математичних наук, доктор юридичних наук, професор, завідувач кафедри кібербезпеки
Національний університет «Одеська юридична академія»
E-mail – nvas08@ukr.net
ID ORCID: http://orcid.org/0000-0002-8555-5712

«SMART CITY» IN THE CONTEXT OF CYBERSECURITY: INCIDENTS, RISKS, THREATS

V. Boyko, M. Vasilenko
National University "Odessa Law Academy", Ukraine

Smart city systems are becoming more and more widespread in the nearest future. Their deployment allows focusing on combining diverse and varied urban information systems into a single sustainable, energy-efficient, low carbon energy, wasteless, clean "ecosystem" which will be friendly and comfortable for its citizens. This system integrates into itself all existing city IT-systems from individual smartphones to complex urban traffic management systems. And the practice shows that the IT-systems of the smart city do not yet sufficiently meet requirements of security and protection from attacks, malware and external threats. In this respect, the Ukrainian epidemic of ransomware WannaCry and Petya presents a good example. It wasn't targeted attack, ransomware wasn't directed or aimed at any of metropolitan or urban infrastructure it-systems, but as a result of collateral damage, more than a third of Ukrainian computer networks (including banking and state ones) were disabled. There is also a significant and growing demand for a targeted attack against industrial and urban infrastructure. Currently, cases of the following attacks are already known and considered in detail: the malicious computer worm Stuxnet which targets industrial systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran and related malware as Duqu and Flame, Triton/Trisis malware which the first appearance was at a petrochemical plant in 2017, and was aimed at attacking the "last line of defense" - safety instrumented systems (SIS) of Schneider Triconex. Thus, it was only a matter of time before smart city faces IT-infrastructure attack. The paper considers sources of threats and the reasons for the weak security of smart city IT-systems including the following: an increase of the attack surface, the lack of a unified strategy and security service, the developers' emphasis on simplicity and ease of systems deployment at the expense of security, a large percentage of wireless technologies that facilitate access to critical infrastructure objects, the presence of obsolete and legacy code sections in the system. The article proposes a set of measures and actions for smart city IT-systems hardening. Also, the paper considers redundancy and inefficiency of old protection methods and measures such as "air gap", proprietary protocols, "secure by obscure" and others.

***Keywords**: smart city, information ecosystems, cybersecurity, municipal economy, risks, threats, incidents, protection.*