МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет
імені Тараса Шевченка

І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

“ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ” (PCSITS)

05-06 квітня 2018 року

Київ – 2018

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431
П 78

П78 Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповодідей та тез; м. Київ, 05-06 квітня 2018 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова) та ін. – К.: ВПЦ «Київський університет», 2018. – 510с.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: українською, російською, англійською.

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431

Київський національний університет імені Тараса Шевченка, 2018

ВСТУП

Завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. **Одн**ак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері. У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх перерахованих системах. Досить велика кількість засобів і систем захисту інформації створюються на основі математичних моделей, з використанням методів цифрової обробки сигналів а також використовують у своїй роботі інтенсивні логічні обчислення.

У збірнику матеріалів науково-практичної конференції опубліковано тези доповідей вчених, науково-педагогічних працівників, аспірантів, студентів Київського національного університету імені Тараса Шевченка та інших вищих навчальних закладів та організацій України, в яких розглядаються науково-технічні та практичні аспекти створення та використання засобів безпеки інформаційно-телекомунікаційних систем та методи управління інформаційною безпекою таких систем.

В роботі конференції взяли участь представники: Київського національного університету імені Тараса Шевченка, Харківського національного університету радіоелектроніки, Одеського національного політехнічного університету, Харківського університету Повітряних Сил імені І. Кожедуба,

Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Державного університету телекомунікацій, Національного авіаційного університету, Державний науково-дослідний інститут спеціального зв'язку та захисту інформації України, Харківського Національного Університету ім.В.Н.Каразіна, ООО «ІТЦ «Хай-Тек Бюро»,Військовий інститут телекомунікацій та інформатизації, АТ «Інститут інформаційних технологій», Військової частини А0515, Національного університету біоресурсів і природокористування України, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Державної наукової установи Інститут модернізації змісту освіти, Державного університету інфраструктури та технологій, Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна, Інституту проблем математичних машин і систем НАН України, Київського університету імені Бориса Грінченко, Одеської національної академії харчових технологій, Чернівецького національного університету ім.Ю.Федьковича, Кавказського університету, Міжнародного чорноморського університету, Національного університету «Львівська політехніка», Національної академії Служби безпеки України, Національної академії внутрішніх справ, Східноукраїнського національного університету імені В. Даля, та інші

СЕКЦІЯ 1.
«НАУКОВО-ТЕХНІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЗАСОБІВ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ»

УДК 004.056

Л.В.Кузьменко[1]
В.Л.Бурячок[2]
[1]*Національна академія Служби безпеки України*
[2]*Київський університет імені Бориса Грінченко*
v.buruachok@kubg.edu.ua

ТЕНДЕНЦІЇ РОЗВИТКУ ТА ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СУЧАСНИХ IOT-ПРИСТРОЇВ

Інтернет речей (IoT) все більше входить в наше життя та розширює можливості платформ і пристроїв. За інформацією Gartner до IoT щодня підключається понад 5,5 млн. нових «речей». Цьому сприяє:

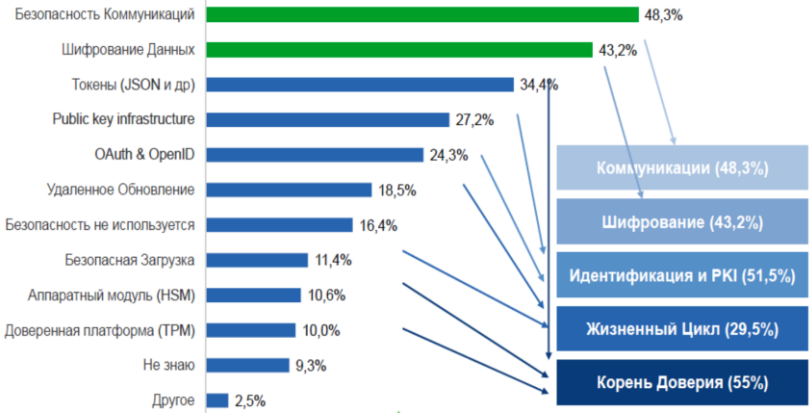
- поширена комунікаційна інфраструктура;
- можливість глобальної ідентифікації кожного об'єкта;
- виняткова здатність кожного об'єкта відправляти і отримувати дані за допомогою персональної мережі, або мережі Інтернет, до якої він підключений тощо.

У 2016 році до IoT було підключено 6,4 млрд.пристроїв. На кінець 2016 року їх загальна кількість досягла 4,9 billion. До кінця 2025 року кількість таких «речей» може збільшитися майже втричі. Як наслідок, за прогнозами Mckinsey Global Institute щорічний економічний ефект від індустрії IoT сягатиме щорічно до 2025 року від 2,7 трлн. до 6,2 трлн.доларів. Переваги від впровадження IoT знайдуть відображення у: зменшенні експлуатаційних втрат; підвищенні операційної ефективності, зменшенні відходів, а також набагато більшій продуктивності не тільки людської праці, а й обладнання.

Разом з тим, поширення IoT тягне за собою й велику відповідальність. Причиною тому є певні «слабкі місця» IoT, що пов'язані з переходом на IPv6, неможливістю забезпечення постійного живлення датчиків, відсутністю стандартизації архітектури і протоколів пристроїв, слабкою аутентифікацією, відсутністю підтримки з боку виробника для усунення вразливостей, неможливістю поновлення ПЗ і ОС, використанням незахищених мобільних технологій та хмарної інфраструктури, використанням небезпечного ПЗ тощо. Саме тому такий стан справ вимагає зосередження уваги, перш за все, на забезпеченні безпеки таких пристроїв на всіх етапах їх життєвого циклу - від створення до

розгортання і після нього. Підтвердженням такому можуть слугувати результати досліджень компанії Raconteur, згідно яких 25% усіх кібератак до 2020 року будуть доводиться на сферу IoT.

Зважаючи, що на поліпшення безпеки бізнес-структур і підприємств нині спрямовується лише до 10% від загальної суми бюджету IT, - стратегії безпеки IoT впроваджено нині лише на 78% у сфері телекомунікацій, на 73% - у сфері інформаційних технологій та на 69% - у сфері транспорту. З цього приводу Gagan Singh, старший віце-президент і генеральний директор департаменту мобільних розробок компанії Avast, відмічає таке: «Мы активно пользуемся устройствами интернета вещей дома и на работе, однако их безопасность до сих пор не идеальна. Это значит, что пользователи и сегодня остаются под угрозой. Ожидания пользователей возрастают: мы хотим получать комфорт и удовольствие от использования умных гаджетов. Поэтому перед производителями встает вопрос обеспечения безопасности умных устройств». Коментуючи стан розвитку власне IoT та засобів їх захисту менеджер корпорації ARM по продуктам IoT Майк Эфтимакіс відмічає таке: «Потенциал устройств IoT и сенсоров огромен. Однако, если мы не сумеем обеспечить безопасность каждого устройства, весьма вероятно, что использование незакрытых уязвимостей остановит прогресс, не позволив нам когда-либо полностью воспользоваться этим колоссальным потенциалом». Головними сферами проблем безпеки IoT-рішень вони, як і більшість інших експертів, вважають:



Основними компонентами захисту середовища IoT при цьому є:

• автентифікація;
• авторизація;
• мережева політика;
• безпечна аналітика: видимість і контроль.

Автентифікаційя. Використовується для надання та перевірки іденти фікуючої інформації об'єкта IoT. Коли підключені пристрої IoT потребують доступу до інфраструктури IoT, довірчі відносини ініціюються на основі ідентифікатора пристрою.

Авторизація. Дозволяє контролювати доступ пристрою по всій мережевій інфраструктурі. Цей рівень ґрунтується на основному рівні аутентифікації, використовуючи ідентифікаційну інформацію об'єкта. З компонентами перевірки автентичності та авторизації встановлюється довірче відношення між пристроями IoT для обміну відповідною інформацією.

Мережева політика. Дозволяє пздіснювати безпечну маршрутизацію всіх елементів IoT та транспортувати трафік кінцевої точки інфраструктурою, будь то управління або фактичний трафік даних. Як і рівень авторизації, вже встановлені протоколи і механізми для захисту мережевої інфраструктури впливають на політику, яка добре підходить для використання IoT.

Безпечна аналітика. Дозволяє визначити служби, за допомогою яких всі елементи (кінцеві точки і мережева інфраструктура, включаючи центри обробки даних) можуть брати участь у забезпеченні телеметрії з метою отримання видимості і, в кінцевому рахунку, контролю екосистеми IoT.

Характерним є те, що окрім захисту власне самих IoT-пристроїв від загроз, необхідно забезпечити й захист даних, що передаються мережею та команд управління, що будуть отримувати такі пристрої

тощо. Головними методами вирішення цих завдань на етапах розробки та експлуатації є передусім забезпечення цілісності коду, що виконується на пристроях та конфіденційності даних (інформації) за рахунок перевірки справжності користувачів і пристроїв, визначення чітких прав володіння для пристроїв (в тому числі даних, створених цими пристроями) та стійкості до віртуальних і фізичних атак.

На етапі розробки	**На етапі експлуатації**
Захист інтерфейсу управління Авторизація користувачів і вбудованого обладнання Обмеження доступності мережевих портів і служб Реалізація крипто захисту на транспортному і канальному рівнях Захист персональних даних, що містить IoT-пристрій Обмеження конфігурування IoT-пристрою користувачем тощо	Сегментація мережі, ізолювання або розділення шлюзами IoT сегментів та критичних сегментів мережі Створення надійних політик безпеки для IoT-пристроїв

Висновок: IoT стає все більш поширеним явищем і все частіше з'являється в системах, від яких залежить життя людей, наприклад, автомобілях, літаках і промисловому обладнанні. IoT спирається на новий стандарт мобільного зв'язку LTE Advanced Pro та відповідне обладнання, що підпадає під обов'язкове підтвердження відповідності. Для IoT-пристроїв необхідно будувати комплексні системи захисту, які були б здатні покрити різні рівні - рівні хмар і підключень.

Література:

1. Адам Тернер. Интернет вещей и носимые технологии : решение тайны частной жизни и безопасности, не сорвать инноваций. – 21 Rich. – JL & Технология. – № 6 (2015), – Режим доступу : http://jolt.richmond.edu/v21i2/article6.pdf;

2. Internet of Things: Privacy & Security in a Connected. – World Federal Trade Commission (FTC) Staff Report. – January 2015. – Режим доступу : https://www.ftc.gov/system/files/documents /reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-priva cy/150127IPrpt.pdf

3. Интернет вещей. – Режим доступу : http://igate.com.ua/tag/ internet-veshhej/4; http://revo lverlab.com/chto-takoe-internet-veschey

4. Интернет вещей : всё подключается к сети. – Режим доступу : http://igate.com.ua/news/ 6309-internet-veshhej-vse-podklyuchaetsya-k-seti

УДК 004.056.53

Д.В.Палко[1],В.І.Вялкова[1],
Л.В.Мирутенко[1]
Київський національний університет імені Тараса Шевченка[1]
palko.dmytro@gmail.com

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ТРАНЗАКЦІЙ В КОРПОРАТИВНИХ МЕРЕЖАХ

Єдиний інформаційний простір на сьогодні являється запорукою успішної діяльності сучасної організації в умовах жорсткої конкурентної боротьби. Саме розвинена інформаційна система є основною передумовою ефективного обігу потоків інформації на підприємстві, що в свою чергу зменшує час реакції на зміни, що відбуваються в компанії, сприяє оперативному прийняттю рішень, і забезпечує оптимальне управління усіма процесами в реальному масштабі часу.

Корпоративна мережа - це складна взаємопов'язана система, що являє собою сукупність мереж і служб передачі даних, які призначені для надання єдиного захищеного мережевого простору обмеженому рамками корпорації колу користувачів.

Такі мережі використовують розподілену модель обчислень. Основними функціональними компонентами корпоративних мереж є робочі місця (абоненти), інформаційні сервери корпорації, засоби телекомунікації, телеслужби, а також різноманітні централізовані системи забезпечення надійності, контролю, діагностики, управління безпекою та ефективністю функціонування. Головною особливістю корпоративних мереж є те, що доступ до інформації надається тільки обмеженій групі осіб у внутрішній мережі організації, що відділена від глобальних мереж брандмауерами. Але при цьому використовується той же

ЗМІСТ