в середовищі IoT. У режимі реального часу й автономних взаємодій між різними вузлами дуже важко або взагалі неможливо визначити масштаби компромісу та межі місця злочину.

Аналіз доказів і кореляція. Більшість вузлів IoT не зберігають жодних метаданих, враховуючи тимчасову інформацію, що робить походження доказів проблемою для дослідника. За відсутності тимчасової інформації, такої як час зміни, доступу та створення, кореляція доказів, зібраних з різних пристрої IoT, практично неможлива. Крім технічних проблем, конфіденційність є основною проблемою, яку слід враховувати під час аналізу та співвіднесення зібраних даних. Більше того, величезному обсягу даних, який збирається в неоднорідних середовищах IoT, майже неможливо надати наскрізний аналіз залишкових доказів.

Всі джерела доказів щодо пристроїв на основі IoT можуть бути поділені на три групи: 1) докази, зібрані з розумних пристроїв і датчиків; 2) докази, зібрані з апаратного та програмного забезпечення, які забезпечують зв'язок між розумними пристроями і зовнішнім світом; 3) докази, зібрані з апаратного та програмного забезпечення, які знаходяться поза межами мережі, що досліджується. До останньої групи входять хмара, соціальні мережі, постачальники послуг інтернету та мобільних мереж, віртуальні онлайн-ідентифікації та інтернет.

Політики хмарної кібербезпеки повинні бути інтегровані з інфраструктурою інтернету речей, щоб швидко реагувати на будь-які підозрілі проблеми діяльності. Політику слід переглянути з точки зору доказів ідентифікації, цілісності, збереження та доступності даних.

Зараз судово-комп'ютерна експертиза і дослідники з кібербезпеки досліджують інтернет речей з точки зору комп'ютерного судового аналітика щодо зібрання даних, вилучення доказів, обробки та аналізу доказів. Докази можуть бути зібрані за допомогою стаціонарних датчиків, що вбудовані у фізичні об'єкти, хмарних сховищ та навіть журналів ISP. Практичне вивчення цієї нової галузі дозволить визначити методи для виконання цифрового криміналістичного аналізу в середовищі IoT.

Таким чином, швидкі темпи розвитку та характер середовищ IoT створюють різноманітні проблеми безпеки та криміналістики. Надані матеріали пропонують сучасний погляд на проблеми конфіденційності, безпеки та криміналістичної експертизи в середовищах інтернету речей, а також інноваційні рішення, які прокладають шлях до безпечного та надійного розгортання мереж IoT.

Одержано 19.04.2022

УДК 342:343.346.8
ГУСАРОВ Сергій Миколайович,
доктор юридичних наук, професор,
заслужений юрист України,
член-кореспондент Національної академії правових наук України,
професор кафедри адміністративного права та процесу факультету № 1
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-8136-0694

ЩОДО РОЗРОБКИ ПОЛІТИКИ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Для того, щоб забезпечити визначені нормативними документами та стандартами принципи управління та підтримку безпеки інформації в конкретній організації, потрібно розробити концептуальний набір правил поведінки, який буде регулювати найважливіші питання, що стосуються безпеки інформації в інформаційних системах. Цей набір правил описує властивості системи, яка потребує захисту, та має назву «Політика безпеки». Політка безпеки формується як окремий документ. Цей документ ухвалюється керівництвом організації та обов'язково доводиться до відома персоналу й інших зацікавлених суб'єктів під підпис. Як правило, політика безпеки затверджується окремим наказом по організації, який на-

лежним чином реєструється. У цьому ж наказі доцільно прописати відповідальність за порушення вимог політики безпеки.

У нормативних документах поняття «політика безпеки» можна зустріти в Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. З урахуванням зазначеного документа *політику безпеки* можна визначити як політику, що визначає підхід підприємства, установи та організації до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки. Політика безпеки є якісним (або якісно-кількісним) описом властивостей захищеності, вираженим у термінах, що описують систему. Саме особливості роботи з інформаційною системою організації складають більшу частину наповнення політики безпеки.

Методичною основою для створення та розробки політики безпеки є стандарти:

– ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;

– ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки».

Форма представлення політики безпеки може бути різною. В окремих випадках її представляють власною назвою, в інших позначають як інструкцію або правила. З точки зору управління безпекою інформації організації, це не повинно мати принципового значення.

Політики безпеки можуть охоплювати:

– всю інформаційну діяльність організації (саме такий вид політики безпеки описаний у стандартах ISO/IEC 27-ї серії);

– конкретну комп'ютерну систему або мережу організації. У цьому випадку часто говорять про вибір однієї з таких політик безпеки, як дискреційна, мандатна, рольова.

Типовими розділами політики безпеки можуть бути:

– вступ або загальні положення;

– терміни та скорочення;

– мета політики;

– сфера застосування;

– предмет документа й опис дій;

– ролі та відповідальність;

– перегляд політики.

У деяких випадках окремим розділом може подаватися перелік взаємопов'язаних документів.

В обов'язковому порядку слід ознайомити з правилами політики безпеки персонал організації, зібрати відповідні розписки. Для підтримання політики безпеки на належному рівні та виконання її всіма працівниками організації потрібно передбачити систему відповідного навчання персоналу, а також порядок і терміни оновлення політики безпеки організації.

Одержано 30.04.2022

УДК 351:343.431

КОБКО Євген Васильович,
кандидат юридичних наук, доцент,
доцент кафедри публічного управління та адміністрування
Національної академії внутрішніх справ
https://orcid.org/0000-0002-3121-0823

НАПРЯМИ ВДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Забезпечення національної безпеки в Україні, особливо в сучасних умовах, є складним процесом, ефективність реалізації якого залежить від того, наскільки уповноважені суб'єкти