Література:

1. Розовский Б.Г. Право как клетка в зверинце / Б.Г. Розовский // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2017. – № 1. – с. 280-292.

2. Карчевський М.В. «Класичні» та новітні проблеми кримінально-правого регулювання у сфері інформатизації / М.В. Карчевський // Актуальні питання кримінального права, процесу і криміналістики, удосконалення діяльності судової і правоохоронної систем : матер. Всеукр. наук.-практ. конф. (м. Сєвєродонецьк, 19 травн. 2017 р.). – Сєвєродонецьк : Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка, 2017. – с. 11- 19.

3. Конашевич О.І. Правові підстави для реалізації послуг та товарів за біткоіни [Електронний ресурс] / О.І. Конашевич – Режим доступу: http://jurliga.ligazakon.ua/blogs_article/725.htm

4. Іванов В. У Швейцарії за 150 років проведено більше 500 референдумів: Блог Владимира Иванова [Електронний ресурс] / Володимир Іванов – Режим доступу: http://blogs.lb.ua/vladimir_ivanov/159889_shveytsarii_150_rokiv_shveytsarii.html

5. "Open Governance and the Definition of e-Democracy"[Електронний ресурс] – Режим доступу: http://www.gov2u.org/index.php/blog/128-open-governance-and-the-definition-of-edemocracy

6. Electronic Voting in Switzerland [Електронний ресурс] – Режим доступу: http://web.archive.org/web/20070212194901/www.swissworld.org/dvd_rom/eng/direct_democracy_2004/content/votes/e_voting.html

7. Direct Democracy [Електронний ресурс] – Режим доступу: http://www.paparty.co.uk

8. В Киеве подписан исторический Меморандум о запуске блокчейн-платформы e-Auction 3.0 [Електронний ресурс] – Режим доступу: http://forklog.com/v-kieve-podpisan-istoricheskij-memorandum-o-zapuske-blokchejn-platformy-e-auction-3-0/

9. В Белой Церкви состоялись торги на e-Auction 3.0 [Електронний ресурс] – Режим доступу: https://bitcoinconf.com.ua/ru/news/v-beloy-tserkvi-sostoyalis-torgi-na-eauction-3-0-52509

10. Блокчейн-сервис электронных петиций e-Vox отобран для участия в инкубаторе EGAP [Електронний ресурс] – Режим доступу: http://forklog.com/blokchejn-servis-elektronnyh-petitsij-e-vox-otobran-dlya-uchastiya-v-inkubatore-egap/

11. Bitcoin против бюрократии: как Украина переходит на блокчейн [Електронний ресурс] – Режим доступу: https://ain.ua/2016/09/14/bitcoin-protiv-byurokratii-kak-ukraina-perexodit-na-blokchejn

12. Подобрій О. В биткоинах есть один негативный момент – ученый из Италии [Електронний ресурс] / О. Подобрій – Режим доступу: https://www.obozrevatel.com/finance/business-and-finance/19048-bitkoinyi.html

Інтернет речей: проблема безпеки

Гончарова Н.І.
кандидат філософських наук, доцент
доцент кафедри філософії та соціально-гуманітарних дисциплін ОДУВС
Гончарова А.В.
студент 2-го курсу ОС «магістр» ІКС ОНПУ

Кінець двадцятого – початок двадцять першого століття позначив для людства певний рубіж, який на сьогодення називають «початком інформаційної революції», і перспективи й збитки якого нам ще доведеться оцінити. Одним із непередбачуваних ефектів інформаційної революції стало те, що розвиток інформаційних технологій, розпочавшись у науковій та промисловій сфері, швидко проник у буденне життя, змінюючи його до невпізнаваності. Звичні побутові пристрої, такі як холодильник, кавоварка чи праска, стали не лише доступними для дистанційного управління, але й взаємопов'язаними, а за деякими функціями – ще й взаємозамінними. Ці пристрої тепер спільно називають «Інтернетом речей» (IoT), і футурологи запевняють, що у найближчому майбутньому вони змінять людське суспільство. Однак окрім полегшення життя «Інтернет речей» несе у собі великі ризики, що досі не набули усвідомлення ані на рівні окремих користувачів, ані на рівні суспільної думки.

Об'єктивним фактором, що обумовлює високий рівень потенційної небезпечності IoT, виступає його належність до високотехнологічних систем, у яких незначні впливи в окремих сегментах можуть спровокувати «ефект доміно» і призвести до значних негативних наслідків. Зокрема, особливо вразливим чинником виступає централізована система управління, оскільки моментний вплив на будь-який елемент цієї системи може привести до руйнування системи в цілому. Іншим небезпечним

сценарієм, що також обтяжений ризиком руйнації системи, є накопичення суми помилок внаслідок нераціональних дій окремих користувачів. У недалекому минулому таким рівнем небезпечності характеризувалися лишень окремі види особливо важливих виробництв та об'єктів, доступ до яких був обмежений. На сьогодення у світі функціонує вже близько 6 млрд. «розумних пристроїв», і з часом їх кількість буде лишень зростати. Отже, існує необхідність досліджень щодо основних видів ризиків, пов'язаних з IoT, і вироблення конкретних методів та заходів їх нейтралізації.

На нашу думку, увесь масив ризиків можна умовно поділити на дві групи: техногенні та антропогенні. Техногенні ризики пов'язані із складністю інтернет-технологій, їх мобільністю та трансформаційністю, а також недостатньою надійністю як окремих технологічних елементів та систем, так і інфраструктур, що забезпечують їх функціонування. До найбільш розповсюджених техногенних ризиків слід віднести:

- недосконале програмне забезпечення та неспівпадіння протоколів обміну інформації між пристроями;
- неякісні деталі, невідповідність елементної бази реальним умовам використання;
- перепади напруги та перерви електропостачання, що тягнуть за собою порушення нормального режиму функціонування та скорочення термінів стабільної роботи гаджетів.

До антропогенних ризиків відносяться ті, що безпосередньо пов'язані із діями користувачів, зокрема:

- відсутність досвіду роботи з «розумними речами», легковажне ставлення до конфіденційності приватної інформації та до можливих наслідків віртуальної діяльності;
- доступність систем для зовнішнього впливу, незалежно від місця знаходження, приватності тощо;
- анонімність та дистанційність впливу;
- доступність інформації про дії користувача в реальному просторі віртуальним спостерігачам (руйнування «зони приватності»);
- *відсутність правового регулювання у цій сфері.*

Усі ці фактори складають підставу для криміногенної та віктимогенної небезпечності IoT, починаючи з продукування та продажі відверто неякісних гаджетів та закінчуючи різними видами фішинга.

Вже на сьогодення відомі неодноразові випадки шахрайства із використанням методів соціальної інженерії, поєднаних із можливостями інтернет-систем (наприклад, звернення із проханням повідомити CVV код платіжної картки - нібито з метою планової банківської перевірки, а насправді – задля зняття коштів з рахунку). Ввійшов у повсякденний вжиток термін «хакерська атака». Широко розповсюджені та мають великий попит нелегальні модифікації програмних кодів та апаратних частин. Має місце специфічний вид тролінгу: свідома пропаганда дій, спрямованих на псування дорогих гаджетів (наприклад, рекомендації зарядити айфон за допомогою мікрохвильової печі або власноруч просвердлити у корпусі роз'єм для навушників). І якщо власник знівеченого айфону принаймні розуміє обсяг своїх збитків (що мають обмежений характер), то ані користувач, ані навіть автор самостійно модифікованих кодів часто не задумуються, до яких наслідків можуть в кінцевому підрахунку призвести їх дії.

Мусимо зазначити, що з розширенням IoT «ефект метелика», коли незначні дії можуть мати великий і непередбачуваний ефект де-небудь в іншому місці та в інший час, може набути глобального характеру. І в цьому плані доводиться говорити про розширення латентного статусу віктимності щодо окремих видів злочинів у сфері інтернет-технологій. Про конкретні наслідки злочинних дій може не знати ані сам злочинець, ані його жертва. Звичайно, потерпілому доводиться мати справу із наслідками злочину, однак він може навіть не здогадуватись, що саме спричинило ці наслідки.

Значущість цієї проблеми з часом зростатиме. Так, дослідження десяти популярних систем безпеки будинків і квартир, проведене компанією HP, показало, що усі вони мали були мали проблеми, пов'язані із захистом паролів, шифруванням і перевіркою автентичності. Усі протестовані хмарні веб-інтерфейси дозволяли потенційному злочинцю отримати доступ до облікових записів, усі збирали певні види персональної інформації, такі як адреси, дати народження, номери телефонів і навіть номери кредитних карток [1], а отже були потенційно віктимогенними системами, що цілком не усвідомлювалось ані їх виробниками, ані користувачами.

Способи нейтралізації вищезазначених ризиків мають відповідно кілька спрямувань:

1. Підвищення надійності систем за рахунок певних технологічних обмежень. Зокрема, до цього напрямку відносяться розвиток і вдосконалення систем «захист від помилки» (чи то «захист від дурня»), що не дають можливості користувачу виконати неправильні дії, або блокують їх наслідки.

Іншим варіантом технологічних обмежень є дублювання систем управління та розподіл їх функцій у такий спосіб, що певні – потенційно небезпечні – способи керування «розумними пристроями» можна здійснити лише знаходячись поруч із приймачем інформації. Наприклад, використач, який підключив праску до «розумної розетки», зможе її вимкнути, знаходячись на будь-якій відстані, а ввімкнути – тільки перебуваючи у безпосередній близькості.

2. Впровадження високих міжнародних та національних технічних стандартів на відповідні технології, які б убезпечували від легального розповсюдження неякісної продукції.

3. Раціональне правове регулювання у сфері інтернет-технологій (яке наразі відсутнє). Профілактика та попередження віктимної поведінки у цій галузі.

4. Формування необхіднодного рівня загальної технічної освіченості.

Однак найважливішим видається інший аспект, що має глобальний характер. На теперішній час людство переживає чергову світоглядну кризу, пов'язану із швидкою трансформацією умов реального життя під впливом інформаційних технологій. Частковим випадком світоглядно-кризових явищ є нерозуміння сучасних можливостей віртуально-реального управління, що стимулює вже усталену безпечність та безкарність віртуальної поведінки. В дійсності межа, що розділяє віртуальний та реальний світи, стає дедалі більш проникною, більш умовною. А віртуальні дії мають цілком реальні наслідки, часом непередбачувані, а періодично - й дуже небезпечні. Подальший розвиток суспільства, та й саме його існування можливе лише за умови формування нового рівня суспільної відповідальності, яка будується на свідомому розумінні безпосереднього зв'язку конкретно-індивідної безпеки та глобальної безпеки людства.

Література:

1. Internet of things research study 2015 report [Электронный ресурс] — Режим доступа: URL: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf . – Назв. с экрана

Формування вимог щодо забезпечення гарантоздатності автоматизованих систем переробки інформації й управління критично-важливими об'єктами інфраструктури

Гулак Г.М.
кандидат технічних наук, доцент
професор СК-31 Навчально-наукового інституту
інформаційної безпеки Національної академії СБУ
Складанний П.М.
аспірант Державного університету телекомунікацій

У сучасному світі спостерігається постійне зростання сфер застосування автоматизованих систем переробки інформації та управління (АСУ) критично-важливими об'єктами інфраструктури (КВОІ), починаючи з енергетики, зв'язку, повітряного та залізничного транспорту й завершуючи високотехнологічними галузями економіки країн світу, як металургійні та хімічні виробництва тощо.

Використання у якості транспортної мережі в АСУ КВОІ глобальної мережі Інтернет підвищує ризики порушення їх гарантоздатності, що включає, зокрема, потенціал виконання визначених завдань, уникаючи можливості непередбачуваних змін системи та послуг, що надаються (властивість цілісності, інакше - імітостійкості), а також неавторизованого доступу до інформації про послуги (властивість конфіденційності).

Слід зазначити, що останнім часом спостерігається стале зростання кількості спроб несанкціонованого втручання в роботу АСУ КВОІ (кібернетичних атак) внаслідок чого органи державного та військового управління, суб'єкти господарювання державного та приватного секторів економіки отримують величезні збитки, а суспільство опиняється на межі як локальних, так і глобальних техногенних катастроф [1]. При цьому, технології та методи забезпечення інформаційної безпеки впроваджуються переважно в автоматизованих системах, у яких обробляється інформація, щодо якої законодавчо визначена відповідальність за реалізацію та дотримання відповідної системи нормативно-організаційних та інженерно-технічних заходів [2].

У той же час, на законодавчому рівні статус інформації, що циркулює у АСУ КВОІ не визначений, відсутні конкретні вимоги та норми щодо її технічного захисту та особливості застосування засобів криптографічного захисту інформації (КЗІ), а питання щодо забезпечення їх гарантоздатності взагалі не розглядається. При цьому в умовах ведення гібридної війни саме АС