Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Чинники кібербезпеки у сучасній Азії

Пядишев В.Г.
кандидат технологічних наук, доцент,
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішнх справ

Напередодні 2018 року спостерігаються грандіозні перегони тенденцій у сфері IT-технологій. Це впливає на почуття свободи людей, створює сумніви в політичному процесі, змінює підходи компаній щодо організації бізнесу. Хоча в решті решт ці або інші тенденції розвитку IT-технологій охоплюють увесь світ, проте вони проявляються в регіонах світу неодночасно, асинхронно. Тому своєчасне їх відстеження в усьому світі надає суб'єктові боротьби з кібер-загрозами певні переваги у часі. Одним з цікавих регіонів, де спостерігається швидкий розвиток як позитивних так і негативних тенденцій в галузі IT-технологій, є Азія.

Загальний стан IT-безпеки в Азії

Протягом останніх місяців у країнах Азії пролунали "попереджувальні дзвінки". У червні масштабна атака з використанням програмного забезпечення для вимагань обрушилася на державні системи, морські порти та багато інших компаній на континенті, паралізуючи операції протягом тривалого періоду часу та вимагаючи від операторів комп'ютерів по 300 доларів США за розблокування систем. Порти в Індії, наприклад, не могли визначити, звідки партії товарів надходять чи куди спрямовуються. Отже, загрози для кібербезпеки є реальними, і вони зростають. Це обумовлює необхідність для урядів, бізнесу та окремих людей готуватися до захисту [1].

Через поглиблення загроз кіберзахисту, багато компаній у всій Азії бачать необхідність вдосконалення кіберзахисту. "Honeywell Process Solutions", одна з провідних компаній цього напряму, співпрацює з Радою з економічного розвитку Сінгапуру з метою створити центр для покращення інновацій у сфері кібербезпеки [2]. Центр не тільки надаватиме аутсорсингові послуги для керованої системи безпеки, але також матиме вдосконалений навчальний центр для розвитку рівня кваліфікації в галузі кібербезпеки в регіоні, а також матиме вельми просунуту сучасну лабораторію щодо досліджень та розробок в галузі кібербезпеки. "Honeywell" є не єдиною компанією в Сингапурі, яка спрямована на підвищення кібербезпеки. Наньянський технологічний університет (Сингапур) звернувся до компанії "GrammaTech", яка займається кібербезпекою в США [3]. Вони працюватимуть разом у напряму покращення пропозицій університету з кібербезпеки. Отже, "GrammaTech" буде надавати найсучасніші статичні та двійкові аналітичні інструменти для підтримки проектів з кібербезпеки.

Крім партнерських відносин, спрямованих на поглиблення досліджень, знань та можливостей в галузі кібербезпеки в Південно-Східній Азії, все більше і більше компаній просто бажають триматися в курсі останніх досягнень у галузі кібербезпеки. Саме для цього в регіоні відбувається декілька конференцій з кібербезпеки, наприклад, конференція "CyberSecurity Asia 2017", яка відбулася в Малайзії [4], або конференція "RSA 2017 Asia Pacific and Japan", яка проходила в Сінгапурі [5]. Компанії та уряди готуються до посилення загроз кібербезпеці. Тобто, ця підготовка вважається абсолютно необхідною. У багатьох з доповідей зазначених конференцій стверджується, що країни Азії не тільки стоять перед найбільшими загрозами для кібербезпеки, але вони також є не найменш підготовленими. Ця комбінація може бути катастрофічною.

Отже IT-захист — це не просто створення безпечного пароля. Кілька переплутаних символів не захистять інформацію. Потрібно більше. Саме це починає враховувати бізнес Азії у всіх своїх практиках та процесах.

Новітні тенденції в галузі IT-безпеки в Азії

Створення нової посади. Зі зростанням кіберзлочинності організації змушені звертати на неї більше уваги. Наразі відповідальність набуває такого рівню, що з нею не може упоратися лише одна IT-команда. З цієї причини, багато компаній прагнуть наймати нових професіоналів або перекласти конкретні обов'язки на нову посаду. Головний службовець з питань кібербезпеки, швидше за все, стане тією позицією, яку потребують більшість великих компаній. На нього буде покладено відповідальність за захист усіх комп'ютерних систем від будь-якої атаки. Окрім запобігання зломам, зазначені професіонали будуть також керувати виправленням ситуації, якщо виникло порушення даних. Вони будуть постійно робити організацію все більш і більш "кібернетично захищеною" [6].

Регуляційні зміни. Просування технології робить необхідними зміни законів та правил. Кібернетичні злочини — це зовсім нова територія, і старі правила не вирішують нову проблему ефективно. У наступному році уряди та організації, ймовірно, почнуть поліпшення або навіть повний перегляд чинних норм, що застосовуються до кібербезпеки. Коротше кажучи, чинні правила цього

моменту створюють помилкове відчуття безпеки для будь-якого бізнесу чи уряду. Якщо кібер-атака трапиться, організації просто не досить моторні, щоб з нею впоратися [7].

Кіберстрахування. Страхування від кібер-ризиків вже існує, але наразі воно просто існує як розширення стосовно інших сучасних ризиків — просте поширення "площі захисту". Проте потрібно більше урахування специфіки. Для забезпечення цієї потреби, напевно з'явиться нова ніша в галузі страхування. Це дасть підприємствам набагато більш конкретні продукти, розроблені з урахуванням унікальних потреб у сфері кібербезпеки. Ці потреби можуть містити все: від покриття витрат на вдосконалення систем та інфраструктури безпеки — до компенсації за втрату довіри та репутації перед нинішніми та потенційними споживачами [8].

Крадіжки витісняються маніпуляціями. Зловмисники починають цікавитись тим, щоб завдавати компаніям довгострокової шкоди. Замість зламування захисту та викрадення даних, вони починають зламувати веб-сайти або бази даних просто для зменшення цілісності даних. Це тип нападу, який завдає шкоди репутації організацій та окремих осіб, що може бути набагато більш шкідливим для компанії, ніж будь-яка тимчасова крадіжка даних [9].

Збільшується складність ушкоджень. Порушення зломи, стають більш ефективними та складними. Чим більше знань хакери одержують стосовно коду, даних та передачі інформації, тим більше хаосу може бути утворено. Вже розроблено програмне забезпечення (віруси) для вимагання та віруси, що викликають експоненціальне наростання ушкодження. І хоча існують способи захоплювати та припиняти розповсюдження цих вірусів, створення непереможного вірусу-вимагача вважається лише справою часу [10].

Підвищення попиту на професіоналів з кібербезпеки. Компаніям задля забезпечення їхньої кібербезпеки слід заздалегідь готуватися до підвищення загроз кібер-атак. Але нинішня глобальна нестача навичок щодо забезпечення кібербезпеки тільки погіршиться. І це, в свою чергу, перетворить організації, які не мають сильних заходів кібер-безпеки, на головну мету хакерів. Ця загроза циклічно зростатиме, що змусить усередині організацій здійснювати вдосконалення навичок та тренінги таким чином, щоб відповідальні за інформаційні технології мали принаймні базові уявлення про те, як забезпечити безпеку даних. Одним словом, навички в галузі кібербезпеки стануть дедалі важливішим чинником протягом найближчих років.

Вдосконалення хакерів. Оскільки зазначене підвищує тиск на хакерів, вони стають більш кмітливими. Вони вивчають глобальні закони про кібербезпеку, з'ясовують нові лазівки, починають організовуватися та об'єднуватися. Деякі з них починають опрацьовувати телефонні центри, щоб узаконити та комерціалізувати свої операції. Інші переміщуються до країн, де легше практикувати кіберзлочини, тобто де слабкі розвідувальні та поліцейські сили. Незалежно від того, чи ховаються вони на великих просторах, або ховаються у невідомих місцях, їхня діяльність не стає менш шкідливою.

IoT безпека. Наразі про багато продуктів з переліку "Інтернет речей" (IoT) заявляють, що вони "безпечні за дизайном" (тобто за своєю суттю). Це гарна ідея, але наразі це неправда. Проте ці продукти, безсумнівно, стають більш безпечними і, до початку 2018 року, можливо, почнуть насправді відповідати цій обіцянці. На жаль, це буде йти рука об руку з більш потужними атаками штучного інтелекту. Автоматизовані зломи стають дедалі більш схожими на ті, що зроблено людиною, і в кінцевому підсумку працівникам служби безпеки буде складно відрізняти поведінки робота-зломника та звичайного користувача [11].

Висновки. Намагаючись створити кібернетично-безпечне суспільство, необхідно, серед іншого, всебічно охоплювати зарубіжний досвід, з одного боку, щодо злочинних тенденцій в галузі IT-технологій, з іншого — щодо й протидії зазначеним тенденціям в усіх зацікавлених галузях: права, IT-технологій, бізнес-менеджменту та інших.

Література:

1. Ransomware cyber attack sweeps globe, India's largest container port in Mumbai hit. *India Today*. June 28, 2017 : site. URL : http://indiatoday.intoday.in/story/petya-ransomware-major-global-cyber-attack-wannacry-jawaharlal-nehru-port-trust/1/988915.html [accessed 02 November 2017].

2. Empie D. Honeywell Invests In Cyber Security Innovation Center In Asia Pacific. *HoneyWell.Com*. June 08, 2017 : site. URL : https://www.honeywell.com/newsroom/pressreleases/2017/06/honeywell-invests-in-cyber-security-innovation-center-in-asia-pacific [accessed 02 November 2017].

3. GrammaTech products to aid NTU's cyber security research. *PR New*s. Jun 20, 2017 : site. URL : https://www.prnewswire.com/news-releases/grammatech-products-to-aid-ntus-cyber-security-research-300475247.html [accessed 02 November 2017].

4. CyberSecurity Asia 2017. Developing a Resilient Guture Ready Organization. 7-8 August 2017, Sheraton Imperial Hotel. URL : https://cybersecurityasia.tech/ [accessed 02 November 2017].

5. RSA Conference. Marina Bay Sands. Singapore. 26-28 July 2017. URL : https://www.rsaconference.com/events/ap17 [accessed 02 November 2017].

6. 10 cybersecurity trends to look out for in 2017. *Information Age*. 16 December 2016 : site. URL : http://www.information-age.com/10-cyber-security-trends-look-2017-123463680/ [accessed 02 November 2017].

7. Cybercrime in Asia: A Changing Regulatory Environment. Marsh and MsLennan Companies. 16 p. URL : https://www.marsh.com/kr/en/insights/research/cybercrime-in-asia-a-changing-regulatory-environment.html [accessed 02 November 2017].

8. XL Catlin launches Cyber and Data Protection Insurance Policy in Asia Pacific. *XL Catlin*. Jul 24, 2017. URL : http://xlcatlin.com/insurance/news/xl-catlin-launches-cyber-and-data-protection-insurance-policy-in-asia-pacific [accessed 02 November 2017].

9. Is data manipulation the next step in cybercrime? *CloudMask*. URL : https://www.cloudmask.com/blog/is-data-manipulation-the-next-step-in-cybercrime [accessed 02 November 2017].

10. Cyber attack: Ransomware cases reported in Asia. *The StraitsTimes: Asia* . URL : http://www.straitstimes.com/asia/east-asia/cyber-attack-ransomware-cases-reported-in-asia [accessed 02 November 2017].

11. Internet of Things (IoT) Security Workshop. *Telefocal Asia*. URL : https://www.telefocal.com/training-course/internet-of-things-iot-security-workshop/ [accessed 02 November 2017]

Щодо питання запобігання і протидії корупції заходами інформаційного впливу

Русс Я.В.
курсант 4-го курсу факультету № 3ОДУВС
Науковий керівник: Ноздрін Д.О.
кандидат юридичних наук
доцент кафедри ОРД факультету № 1 ОДУВС

Запобігання корупції – це стратегічний напрям антикорупційної політики будь-якої держави. В умовах інтеграції України з європейським та світовим товариством одним із важливих аспектів сучасної державної правової політики є реформування та вдосконалення системи запобігання та протидії корупції, тому із основних напрямів сучасної стратегії розвитку України є прагнення до подолання корупції та її суспільно-політичних наслідків. Міжнародною інтеграцією визнано, що корупція є досить глобальною проблемою будь-якої країни. Корупція – багатоаспектне соціально-економічне, політичне, правове та морально-етичне явище, яке складається з комплексу протиправних дій і неетичних вчинків, яке завдає істотної шкоди нормальному функціонуванню моральних та правових відносин у суспільстві й державі. Аналізуючи міжнародний досвід з протидії корупції можна стверджувати, що корупція це саме той негативний чинник, який створює реальну загрозу національній безпеці та демократичному розвитку більшості країн світу та негативно впливає на всі сторони суспільного життя. Чинники успішної протидії корупції вже давно відомі та апробовані зарубіжними країнами. Корупція, як негативне явище, притаманне будь-якій державі та будь-якому суспільстві, на сьогоднішній день не існує держави, яку б можна оголосити вільною від корупції. Але такі країни як Фінляндія, Данія, Сінгапур, Швеція, Канада, Нідерланди та інші стали досить «чистими» з точки зору корупції (за рейтингом корумпованості), оскільки вони створили найбільш ефективний механізм протидії корупційним проявам [1, с. 64]. Зазначені країни мають деякі особливості в організації антикорупційної діяльності, але спільними рисами для подолання корупції було: бажання організації активної протидії корупційним проявам; створення відповідної нормативно-правової бази; залучення до протидії корупційним проявам громадських організацій, використання інформаційних заходів для подолання корупції.

В Україні корупція завдає шкоди найбільш важливим сферам суспільства і держави, що негативно впливає на політичні, соціально-економічні, правові та інші цінності, породжує соціальну напругу, безсилля, беззахисність, відчуття обману й розчарування громадян до публічних владних структур. За останні роки в Україні було зроблено чимало кроків для запобігання корупції: було прийнято нове антикорупційне законодавство, з’явилася низка нормативно-правових актів, які спрямовані саме на запобігання і протидію корупції. Україна почала тісно співпрацювати з