УДК 004.056.53

Романюк О. Н., д-р. техн. наук, професор,
завідувач кафедри програмного забезпечення,
Борисова К. О.
Вінницький національний технічний університет

АНАЛІЗ ОСТАННІХ ЗЛОВМИСНИХ ДІЙ У КІБЕРПРОСТОРІ

Кількість даних невпинно зростає: з 2010 по 2020 рік обсяг інформації, що зберігається, збільшився у 50 разів [1]. Особливо важливою інформація стає в контексті її обробки з допомогою сучасних технологій. Чим більш цінною є інформація, тим більше вона потребує захисту. Важливою задачею є мінімізація шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [2].

Крадіжка особистих даних, викрадення грошових коштів з рахунків клієнтів банку, знищення сайтів (повне видалення або блокування) – це лише частина проблем, з якими зіткнулися сучасне суспільство і бізнес.

Атака хакерів, що була здійснена на найбільший агрегатор кредитної звітності в США Equifax, в повній мірі продемонструвала, до чого призводить витік інформації у великій компанії. Зловмисникам вдалося отримати 147 мільйонів імен і дат народження, 209 тисяч номерів карт із зазначенням терміну їх дії, а також близько 145 мільйонів номерів соціального страхування. Витік персональних даних стався в 2017 році, а в липні 2019 року Федеральна торгова комісія США оголосила, що компанія погодилася виплатити майже $ 700 млн в рамках міжнародної угоди. Таку рекордну суму довелося виплатити тому, що компанію звинуватили в недотриманні основних запобіжних заходів, які могли б запобігти витоку даних. [3]

У 2015 році об'єктом зловмисних дій у кіберпросторі стали офіційні листи та особисті дані політика Ангели Меркель [4]. Незадовго до інциденту з канцлером парламент Німеччини піддався масштабній хакерській атаці, після якої багато документів парламентської комісії з'явилися на сайті WikiLeaks. За даними влади, зловмисник отримав доступ до двох облікових записів електронної пошти канцлера, що містить повний трафік листів з 2012 по 2015 рік.

У 2020 році зловмисники отримали доступ до персональних даних кількадесят тисяч пацієнтів мережі психологічних клінік Фінляндії, Vastaamo [5]. Конфіденційна інформація про пацієнтів була частково опублікована в даркнеті, а з деякими клієнтами Vastaamo хакери і зовсім

зв'язалися безпосередньо. Сама компанія повідомляла про злам її інформаційної системи двічі: в листопаді 2018 та березні 2019 року.

Можна зробити висновок, що в сучасному світі хакерські атаки можуть мати вплив як на великі корпорації, так і на життя політиків і звичайних людей. Наступна видозміна кібератак має всі шанси впливати на життєдіяльність і здоров'я людини.

З 2014 року появилися розумні пристрої і девайси: розумні холодильники, фітнес браслети, шоломи віртуальної реальності, окуляри доповненої реальності. З 2018 року розпочали активно імплантувати чіпи, які б замінювали ключі, карти, ідентифікаційні дані, а в 2019 році проєкт "xNT" почав розсилку чіпів для імплантації в руку своїм покупцям. Apple заснували тенденцію на FaceID, завдяки якій можна здійснювати покупки і ідентифікувати людину просто по обличчю [6]. Дані винаходи свідчать про те, що апаратура стає ближче до тіла людини, що створює великий ризик кібератак, які можуть вплинути на фізичний стан людини.

Підводячи підсумки, можна констатувати, що безпека даних наразі залежить від захисту процесів, інформації та діяльності в кіберпросторі. Відсутність заходів кібербезпеки може призвести до порушення конфіденційності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дядкін М. Что такое кибербезопасность и почему за этой профессией будущее? Режим доступу: https://proglib.io/p/chto-takoe-kiberbezopasnost-i-pochemu-za-etoy-professiey-budushchee-2020-07-20

2. Про тлумачення та визначення поняття «кібербезпека». Режим доступу: http://ippi.org.ua/sites/default/files/14boavpk.pdf

3. Sephton C. Самые крупные утечки данных в бизнесе за последние годы. Режим доступу: https://currency.com/ru/major-data-breaches

4. Российские хакеры взломали электронную почту Ангелы Меркель – Spiegel. Режим доступу: https://www.eurointegration.com.ua/rus/news/2020/05/8/7109694/

5. Нефьодова М. В Финляндии взломан психотерапевтический центр. Данные пациентов опубликованы в даркнете. Режим доступу: https://xakep.ru/2020/10/27/vastaamo/

6. Інформаційна безпека і кібербезпека – в чому різниця? Режим доступу: https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Національний технічний університет України
«Київський політехнічний інститут» ім. І. Сікорського
Інституту кібернетики ім. В.М. Глушкова НАН України,
Інституту телекомунікацій і глобального інформаційного простору НАН України
Інститут інформаційних технологій і засобів навчання НАПН України
Житомирський державний університет ім. Івана Франка,
Житомирський військовий інститут імені С.П. Корольова
Shantou University (Китайська Народна Республіка)
Luleå university of technology (Королівство Швеція)
Politechnika Opolska (Poland)
Warsaw University of Technology (Poland)
Технічний університет (Чеська Республіка)
Технічний університет (Республіка Болгарія)
Університет країни Басків (Іспанія)
Віденський технічний університет (Австрія)

ТЕЗИ ДОПОВІДЕЙ

XII Міжнародної науково-технічної конференції

Інформаційно-комп'ютерні технології – 2021 (ІКТ-2021)

м. Житомир, 01-03 квітня 2021 р.

Житомир
2021

УДК 004
ББК 32.97
Т11

Рекомендовано до друку Вченою радою Державного університету «Житомирська політехніка» (протокол № 5 від 20 квітня 2021 р.)

Т11 **Тези** доповідей XII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2021 (ІКТ-2021)», м. Житомир, 01 - 03 квітня 2021 р. – Житомир: Житомирська політехніка, 2021. – 205 с.

Представлено доповіді учасників XII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2021 (ІКТ-2021)». Наведено аналіз та результати досліджень сучасних проблем інформаційних технологій, математичного моделювання та розробки програмного забезпечення, комп'ютерної інженерії та кібербезпеки, інформаційних систем, телекомунікацій, інформаційних технологій в медицині, використання інформаційно-комунікаційних технологій в освіті, цифрової обробки сигналів, комп'ютерно-інтегрованих технологій, приладобудування.

УДК 004
ББК 32.97

Секція 3. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Наукове видання

Тези доповідей XII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2021 (ІКТ-2021)»

Автори несуть повну відповідальність за зміст поданих тез конференцій.

Відповідальний за випуск: Надія ЛОБАНЧИКОВА