СЕКЦІЯ 5
ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА ЯК ОСНОВА ЗМІЦНЕННЯ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

КІБЕРЗЛОЧИННІСТЬ У ФІНАНСОВІЙ СФЕРІ УКРАЇНИ

Вінницька О. А,. *к. е. н., доцент*
Чолинець Я. В., *студентка*
Уманський державний педагогічний університет імені Павла Тичини

Питання кібербезпеки завжди були дуже актуальними в різних сферах людської діяльності в усьому світі, оскільки шкідливі програми, запроваджені в мережі державних і комерційних структур, банків, конкуруючих фірм та різних суб'єктів, а також інші види кіберзлочинності з кожним роком завдають усе більшої шкоди. Її обсяги обчислюються мільярдами доларів, а прибутки від такої діяльності знаходяться на рівні прибутків від торгівлі зброєю чи наркотиками. Більше того, останнім часом з'явився особливий вид програм, які за своїми функціональними характеристиками належать до кіберзброї, і за їх створенням стоять навіть державні структури. Тому гарантування кібербезпеки є одним із головних аспектів національної безпеки кожної країни.

Для таких злочинів використовується й соціальна інженерія, яку в наш час активно експлуатують в Інтернеті з метою отримання закритої інформації чи такої, яка має велику цінність. Її зловмисник одержує, наприклад, шляхом збору інформації про службовців об'єкта атаки за допомогою звичайного телефонного дзвінка або шляхом проникнення на їхні інтернет-сайти [1].

Не працюють банкомати, термінали самообслуговування, пропадає мобільний зв'язок та Інтернет. Це змушує різного роду злочинців, у тому числі й хакерів, мігрувати в інші регіони, де немає війни, а також удосконалювати методи інтернет-шахрайства та психологічного впливу на клієнтів банків. І хоча в цілому зростання кількості злочинних дій у банківській сфері не спостерігається, ситуація контрольована, та суспільна небезпека таких злочинів залишається дуже великою [2].

Актуальність посилення заходів кібербезпеки в банківській сфері пов'язана також і з тим, що банківські технології масово переміщуються у сферу безконтактних платежів у вигляді дистанційного банківського обслуговування. Клієнти мають можливість здійснювати платежі й отримувати грошові перекази в мережі Інтернет без використання платіжної картки, шляхом обміну SMS повідомленнями з банком і з використанням інших сучасних, зокрема й інтернет-технологій.

З одного боку, це полегшує клієнту доступ до банківських послуг, а з другого – робить його вразливішим до різного роду кіберзлочинів. Тому кожен банк повинен приділяти захисту своїх клієнтів, а також власної бази велику увагу, як це робиться в банках, де застосовують спеціальні антивірусні та інші

програми, новітні технології. Банківська захищеність важлива для стійкості всієї банківської системи України і водночас є складовою частиною системи національної безпеки нашої держави, вони значно посилили свою кібербезпеку в воєнний період, щоб не дати ворогові можливості підірвати валютно-фінансову систему держави [3].

Тому слід нагадати, що не потрібно розголошувати дані про ПІН-код платіжної картки, термін її дії, тризначний код CVV2/CVC2, нанесений на її тильній стороні, який використовується для перевірки достовірності платіжної карти при оплаті через Інтернет і інших видах операцій. Нікому не можна повідомляти дані, які надійшли з банку в SMS-повідомленнях, а тим більше під впливом сторонніх осіб уводити отримані в них конфігурації цифр або літер у банкоматах, терміналах чи в мобільних додатках смартфонів. Неприпустимо переходити за посиланнями, які надходять на смартфони клієнтів, адже хитрість кібершахраїв полягає в тому, що вони надсилають їх із телефонів, які викликають довіру, а насправді поширюються через інші, заражені вірусами, смартфони [7].

Атаки часто проводять на веб-сайти великих банків, у яких немає належного захисту. За даними експертів, нині чотири із п’яти банківських ресурсів є вразливими, а три з чотирьох атак здійснюються через незахищені додатки, причому одна маленька вразливість може становити загрозу для цілої фінансової організації. Останнім часом кіберзлочинці активно використовують мобільні технології. Більшість мобільних шкідливих додатків орієнтована передусім на крадіжку грошей – нині явно простежується “банківська” спрямованість розвитку мобільних злочинів [4].

Творці вірусів стежать за розвитком сервісів мобільного банкінгу і за успішного інфікування смартфона відразу перевіряють, чи прив’язаний він до банківської карти. Згідно з даними за 2013 рік Україна входить до трійки світових лідерів за кількістю заражених мобільних пристроїв. Її частка у світовому показнику таких пристроїв становить 5,9%. У 2012 році з банківських рахунків у нашій країні було викрадено 11.4 млн. грн. (в основному при проведенні грошових розрахунків у системі інтернет-банкінгу чи на сайтах торгово-роздрібних мереж) [5].

Для ефективного захисту від кіберзлочинності необхідно вдосконалити і доповнити законодавчу базу та національні стандарти у сфері кібербезпеки, а також розробляти програми, які гарантують кібербезпеку фінансових структур і громадян, та системи управління інформаційною безпекою і протидії кібертероризму.

Слід впроваджувати передовий досвід зарубіжних країн у цій сфері. Регулярно проводити інвентаризацію та аналіз вразливості систем захисту від кіберзлочинів, а також аудит ІТ-процесів, який дасть змогу точно оцінити стан ІТсистеми, виявити ризики та отримати рекомендації щодо їх усунення. Постійно контролювати персональну техніку співробітників фінансових установ, які працюють у корпоративній мережі з конфіденційною інформацією. Їхній низький рівень комп’ютерної грамотності та незнання можливих варіантів

кіберзагроз є однією з причин заражень комп'ютерів вірусами та витоку інформації [6].

Тому варто постійно проводити навчання персоналу. Зважаючи на те, що кількість кібератак зростатиме, слід приділити увагу превентивним способам захисту банків". Учасники круглого столу внесли пропозиції щодо вироблення елементів концепції розвитку кібербезпеки в Україні, розгляду можливості створення спеціального національного науково-освітнього центру та робочої групи з розробки декларації чи меморандуму з розвитку кібербезпеки, які б лягли в основу законодавчих ініціатив. Крім того, наголошували виступаючі, необхідно розвивати внутрішній ринок розробок із кібербезпеки всіх структур, зокрема й банківських, а не орієнтуватися на аутсорсинг. Особливу увагу слід приділити стандартизації безпеки, а також створити перелік понять і класифікатор, використовуючи міжнародний досвід. Зважаючи на важливість питання та велику кількість проблем із кібербезпеки, було запропоновано частіше розглядати їх у якомога ширшому колі фахівців.

Список використаних джерел:

1. Государственные стратегии кибербезопасности [Електронний ресурс] URL: http://www.bezpeka.com/ru/lib/sec /government-cybersecurity-strategy. html

2. Европа объявила войну киберпреступности. [Електронний ресурс] URL: http://www.dw.de/европа-объявила-войну-киберпреступности/a-15988857-1

3. Европейская Конвенция по киберпреступлениям от 23 ноября 2001 г. [Електронний ресурс] URL: http://www.eos.ru/eos_delopr/eos_law /detail.php?ID= 32003&SECTION_ID=671

4. Европейский центр борьбы с киберпреступностью отчитался за первый год работы. [Електронний ресурс] URL: http://www.interfax.ru/world/357250

5. Кримінальний кодекс України. [Електронний ресурс] URL: http://zakon4. rada.gov.ua/laws/show/2341-14

6. Курносов И.Н. Информационное общество и глобальные информационные сети: вопросы государственной политики. Информационное общество, 1998, вып.6, с. 29 –36.

7. Про ратифікацію Конвенції про кіберзлочинність: закон України від 7 верес. 2005 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5-6. Ст. 71

ОРГАНІЗАЦІЙНІ ЗАХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Дубичинська К. О., *магістрантка*
Науковий керівник: к. е. н., доцент *Тардаскіна Т. М.*
Одеська національна академія зв'язку ім. О. С. Попова

В наш час одним з найцінніших ресурсів є інформація. Саме тому надзвичайно багато уваги приділяється її захисту. В процесі створення та