Хмилівська Ю. В., курсант 3-го курсу навчально-наукового інституту № 1 Національної академії внутрішніх справ
Науковий керівник: старший викладач кафедри інформаційних технологій та кібернетичної безпеки Національної академії внутрішніх справ, кандидат юридичних наук ***Чукаєва А. В.***

СОЦІАЛЬНА ІНЖЕНЕРІЯ: ЗВ'ЯЗОК ІЗ СИСТЕМОЮ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

В умовах науково-технічного прогресу інформація стає об'єктом специфічних суспільних відносин, що виникають із моменту її створення, у процесі накопичення, зберігання, обробки та використання, набуття товарного вигляду. Однак застосування сучасних інформаційних технологій, крім позитивних здобутків, означена потенційною можливістю щодо використання сучасних комп'ютерних технологій із корисливою метою. Інтенсивне впровадження автоматизованих систем в економіці, управлінні та особливо кредитно-банківській діяльності зумовило виникнення нового класу злочинців – злочинців у галузі комп'ютерної інформації або комп'ютерних злочинів.

Соціальна інженерія – це метод несанкціонованого доступу до інформаційних систем, який був заснований на особливостях психологічної поведінки людини.

На нашу думку, це поняття слід розглядати в декількох аспектах. Отже, соціальна інженерія – це метод несанкціонованого доступу до інформації або системам зберігання інформації без використання технічних засобів. Метод ґрунтується на використанні слабкостей особистості людини і є досить ефективним. Зловмисник отримує інформацію, наприклад, шляхом збору інформації про службовців об'єкта атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця. Зловмисник може зателефонувати працівникові компанії (під виглядом технічної служби) і вивідати пароль, пославшись на необхідність розв'язання незначної проблеми в комп'ютерній системі. Досить часто цей

трюк має успіх. Найсильніша зброя в цьому разі – приємний голос та акторські здібності зловмисника. Сприяє реалізації таких дій навіть дослідження сміттєвих контейнерів організацій, віртуальних сміттєвих кошиків, крадіжка портативного комп'ютера та інших носіїв інформації.

Для аналізу ефективності боротьби із соціальною інженерією як одним із проявів кіберзлочинності необхідно ознайомитися із основними способами її застосування на практиці.

Фішинг – техніка, спрямована на неправомірне отримання конфіденційної інформації. Зазвичай зловмисник посилає на електронну пошту підроблений під офіційний лист – від банку або платіжної системи – вимагає «перевірки» певної інформації або вчинення певних дій. Цей лист зазвичай містить посилання на фальшиву веб-сторінку, яка імітує офіційну, з корпоративним логотипом і наповненням, і містить форму, що вимагає ввести конфіденційну інформацію – від домашньої адреси до пін-коду банківської картки.

Вішинг. Назва цього виду інтернет-шахрайства пішла від попереднього та полягає в імітуванні дзвінків на мобільний телефон, ніби від банківської установи (із попередньо записаним голосом) та отриманні запиту про комунікацію із банком для підтвердження тієї чи іншої інформації. Причому жертва отримує вимогу сказати свій пароль або іншу конфіденційну інформацію, яка необхідна для доступу до банківських рахунків.

Фармінг. Процедура полягає в перенаправленні жертви на неправдиву IP-адресу. Шахрай встановлює на комп'ютерах шкідливу програму, яка після запуску на комп'ютері здійснює перенаправлення жертви замість потрібних їй сайтів на підроблені.

Попередження про вірус на комп'ютері. У цьому разі розробник шкідливого програмного забезпечення попереджає жертву про зараження її комп'ютера вірусом і повідомляє, що для очищення операційної системи необхідно перейти за посиланням та встановити необхідну програму. Саме ця програма є шкідливою та забезпечує доступ до необхідної інформації.

Кви про кво. Цей вид інтернет-шахрайства ґрунтується на вмінні особи в телефонній розмові або електронною поштою увійти в довіру до жертви (зазвичай офісного працівника) та, представившись співробітником служби технічної підтримки, запропонувати розв'язати проблему, отримуючи таким чином необхідну конфіденційну інформацію.

«Дорожне яблуко». Цей спосіб шахрайства ґрунтується на використанні фізичних носіїв інформації. Так, шахрай може залишити в будь-яких публічних місцях флеш-носій, CD-диск із таким зображенням, яке може зацікавити жертву та примусити її переглянути на своєму комп'ютері.

Зворотна соціальна інженерія. Реалізація цього способу може бути здійснена лише в разі, коли шахрай попередньо знайомий із жертвою та заслуговує на її довіру. У такому разі жертва сама звертається до шахрая (наприклад, системного адміністратора) із проханням допомогти відновити втрачений файл (який заховав сам шахрай). Причому їй повідомляють, що таку дію можна зробити якнайшвидше лише зайшовши в її обліковий запис. Таким чином, жертва за власним бажанням повідомляє всю інформацію шахраю.

Претекстинг – атака, для здійснення якої шахрай представляється іншою особою та дізнається в жертви всю необхідну інформацію. Однак такий вид інтернет-шахрайства вимагає дуже якісної підготовки та збору всієї необхідної попередньої інформації про особу.

Політика безпеки ґрунтується на аналізі поточного стану й перспектив розвитку інформаційної системи, можливих загроз і визначає: мету, задачі та пріоритети системи безпеки; галузь дії окремих підсистем; гарантований мінімальний рівень захисту; обов'язки персоналу із забезпечення захисту; санкції за порушення захисту.

Якщо провадження політики безпеки є непослідовним, імовірність порушення захисту інформації суттєво зростає. Захистом інформації вважають комплекс заходів, який забезпечує:

– збереження конфіденційності інформації – запобігання ознайомленню з інформацією невповноважених осіб;

– збереження інформації – запобігання пошкодженню чи знищенню інформації внаслідок свідомих дій зловмисника, помилок персоналу тощо;

– прозорість (наявність системи безпеки не має створювати перешкод для нормальної роботи системи).

Існує декілька правил, які допомагають не стати ошуканим:

– звертати увагу на написання адрес сайтів;

– якщо пропонують переглянути сайт/фото/відео, зазиваючи емоційними закликами – не переходити одразу;

– уводячи логін/пароль в акаунтах на сайтах, звертати увагу на незвичайні зміни зовнішнього вигляду сторінок (якщо щось викликає підозру – повторно перевірити оригінальність ресурсу);

– критично ставитись до електронних листів, особливо до посилань, за якими пропонують перейти незнайомі відправники повідомлень.

Передусім слід акцентувати на тому, що 2016 року відбулися зміни у сфері боротьби із кіберзлочинністю загалом, оскільки Президент України підписав Указ, яким увів у дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України».

У документі наголошено, що разом із перевагами сучасного цифрового світу та розвитком інформаційних технологій нині активно розповсюджуються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об’єктах інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет. Аналіз цього документа дає змогу викласти такі його основні положення:

1. Виявлено основні загрози кібербезпеці України та згадано Російську Федерацію як потенційне джерело таких загроз, а також описано їх чинники;

2. Закріплено основні завдання Національної системи кібербезпеки, зазначено відповідні органи та сферу їх відповідальності;

3. Визначено основні пріоритети й напрями забезпечення кібербезпеки України (одним із них є проведення навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі).

Крім цього, Указом Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації"» від 13 лютого 2017 року № 32/2017 введено в дію зазначене рішення РНБО. У цьому рішенні звертається увагу на найбільш важливі кроки щодо захисту об'єктів критичної інфраструктури від кіберпосягань, а також вимоги до Кабінету Міністрів України щодо розробки законодавчих пропозицій по імплементації положень Конвенції про кіберзлочинність.

Ці акти переважно спрямовані на утвердження засад вивчення і встановлення потужної системи кібербезпеки України, однак лише незначна кількість їхніх положень можуть стосуватися кібербезпеки приватних осіб. Серед іншого, це зумовлено політичною ситуацією в країні, проте, на нашу думку, зважати на інтереси громадян України та інших осіб слід навіть в умовах нестабільної ситуації в Україні.

Одним із небагатьох кроків, які дають змогу стверджувати, що в Україні щось реально здійснюється в напрямі підвищення рівня кібербезпеки, окрім прийняття стратегій та декларацій, є прийняття 20 вересня 2016 року за основу в першому читанні проекту Закону України «Про основні засади забезпечення кібербезпеки України». Вважаємо за доцільне проаналізувати його окремі положення в контексті забезпечення захисту від проявів соціальної інженерії для приватних осіб.

Увагу привертає те, що поняттям «кібератака» можна позначати також несанкціонований доступ до конфіденційної інформації приватної особи. Це, безперечно, є позитивним аспектом. Одним з основних напрямів забезпечення кібербезпеки України є підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі.

Можна дійти висновку про важливість ролі соціального інжинірингу та підготовки досвідчених фахових спеціалістів, що нині є затребуваними в більшості організацій та компаній. Також доцільно враховувати зарубіжний досвід упровадження соціального інжинірингу та його імплементації як інструменту й гарантії сталого розвитку. Ключовими недоліками у сфері запобігання негативним проявам соціальної інженерії залишаються брак системної роботи з цього питання, низький рівень поінформованості населення стосовно можливих загроз соціальної інженерії, а також висока латентність злочинів у цій сфері, що унеможливлює виявлення та притягнення до відповідальності всіх винних осіб.

Лесик Я. В., курсант 3-го курсу навчально-наукового інституту № 1 Національної академії внутрішніх справ
Науковий керівник: професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук ***Марков М. М.***

НЕЛЕГАЛЬНА МІГРАЦІЯ ЯК НЕГАТИВНЕ ЯВИЩЕ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Геополітичні трансформації впливають на всі аспекти життя суспільства, зокрема й на міграційні процеси. Інтенсивність, характер, спрямованість міграційних настроїв населення України особливо змінилися після розпаду СРСР та здобуття незалежності. Інтеграція України в ЄС спричинила провадження низки важливих реформу у сфері міграційного регулювання.

Географічне положення нашої держави зумовлене близьким розташуванням до країн походження нелегальних мігрантів. У цьому аспекті нелегальна міграція стає однією з головних загроз національній безпеці України. Знання та розуміння реальної ситуації вчинення злочинів, пов’язаних із нелегальною міграцією, необхідне для визначення як державної