

уровнем со стороны уровня U_i , находящегося в состоянии x , выражается равенством $\psi_{ij}(x) = Z_j$.

Отображения φ_i и ψ_i определяют приоритетность уровней. Действительно, при определении значения $\varphi_i(x)$ (соответственно $\psi_i(x)$) ($x = (x_1, x_2, \dots, x_n)$) прежде всего учитываются элементы множества $\varphi_{1i}(x_1)$, затем $\varphi_{2i}(x_2)$ и т.д. до $\varphi_{ni}(x_n)$ (соответственно $\psi_{1i}(x_1)$, $\psi_{2i}(x_2)$, ..., $\psi_{ni}(x_n)$).

Сохраняя принятую индексацию, мы будем говорить, что уровень U_k является вышестоящим по отношению к U'_k , если $k < k' (U_k > U'_k)$. Следовательно, можно говорить об упорядоченном множестве уровней системы U , где $U_1 > U_2 > \dots > U_n$, взаимосвязь которых как сверху вниз, так и снизу вверх характеризуется функциями φ_{ij} и ψ_{ij} ($i, j = 1, 2, \dots, n$) и не ограничивается при этом взаимодействиями между соседними уровнями.

Состояние x системы U будем называть идеальным (или решение системы), если x является неподвижной точкой многозначного отображения φ , т.е. $x \in \varphi(x)$. Если множество неподвижных точек отображения φ не пусто ($F_{ix}\varphi \neq \emptyset$), то система U называется разрешимой.

Иерархическая система потенциально управляема в состоянии x , когда существует такое управление $z \in \psi(x)$, что $z(x) \in \psi(z(x))$, и полностью управляема в состоянии x , если $\forall \omega \in \Omega \exists z \in \psi(x)$, то $z(\omega(x))$ – неподвижная точка отображения φ .

В общем случае под управлением иерархической системы можно понимать конечную последовательность управлений $z_1, z_2, \dots, z_p$, которая приводит состояние x системы в состояние x_p так что $z_i(x) = x_1$, $z_l(x_{l-1}) = x_l$ ($l = 1, 2, \dots, h$).

Если ввести в рассмотрение функцию $f: Z \rightarrow R$ множества Z во множество действительных чисел, то можно говорить, например, о „стоимости” управлений и решать задачу об оптимальном управлении в иерархических системах.

Для разрешимости системы U необходимо, чтобы ($F_{ix}\varphi_{11} \neq \emptyset$). Действительно, если $x = (x_1, x_2, \dots, x_n)$ – неподвижная точка отображения φ , то $x_1 \in \varphi_1(x)$.

В силу определения φ_1 равно $\varphi_1(x) \cap \varphi_{11}(x_1) \neq \emptyset$ и $\varphi_1(x) \subseteq \varphi_{11}(x_1)$, следовательно $x_1 \in \varphi_{11}(x_1)$. Пусть $x_1, x_2, \dots, x_n$ являются непустыми компактными выпуклыми множествами в банаховых пространствах $X_1, X_2, \dots, X_n$. Тогда для того, чтобы иерархическая система была разрешимой, достаточно, чтобы отображение φ_{ki} ($1 \leq i, k \leq n$) были замкнутыми и выпуклыми.

Действительно, при этих условиях множество состояний X иерархической системы является компактным выпуклым множеством в банаховом пространстве $x = \prod_{i=1}^n x_i$. В силу

определения отображений φ_j ($j=1,2,\dots,n$) для всех $x \in X$ $\varphi_j(x)$ непусто и для каждого j

$$\exists_k : \varphi_j(x) = \bigcap_{i=1}^k \varphi_{ij}(x),$$

поэтому для всех $\varphi_j(x)$ является замкнутым и выпуклым как непустое пересечение выпуклых множеств. Тогда отображение $\varphi = \bigtriangleup_{j=1}^n \varphi_j$ будет удовлетворять условиям замкнутости и компактности. И по теореме Какутани о неподвижных точках имеем: $F_{ix}\varphi \neq \varphi$.

Предложены новые показатели эффективности системы управления производством. Разработанные подходы к алгоритмам автоматизированного синтеза структуры иерархической системы управления производством обеспечивают снижение временных и денежных затрат, способствуют скорейшему переходу к внедрению системы на конкретном производстве.

Литература

1. Иванов В.В. Обзор достижений в области кибернетики и вычислительной техники: Вопр. точности и эффективности вычисл. алгоритмов, - Киев: ИК АН УССР, 1969. – 135 с.
2. Монтгомери Д.К. Планирование эксперимента и анализ данных: Пер. с англ.-Л. : Судостроение, 1980. – 384 с.
3. Справочник по типовым программам моделирования / А.Г. Ивахненко, Ю.В. Коппа, В.С. Степашко и др.; Под ред. А.Г. Ивахненко. - К.: Техніка, 1980. – 184 с.
4. Месарович М., Такахара М. Общая теория систем: математические основы . - М.: Мир, 1987. – 311 с.
5. Александров В.В., Горский Н.Д. Алгоритмы и программы структурного метода обработки данных. Л.: Наука, 1983. – 288 с.

ФШИНГ ЯК СУЧАСНА ПРОБЛЕМА СУСПІЛЬСТВА

Міленьєва А.М.

*слухач 2-го курсу магістратури факультету № 1
Одеського державного університету внутрішніх справ*

Ісмайлов К.Ю.

*кандидат юридичних наук, майор поліції
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ*

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів

комунікацій. На сьогоднішній день спостерігається поширення злочинності з використанням глобальної інформаційної мережі Інтернет. Окремим питанням кіберзлочинності присвячено роботи як вітчизняних, так і зарубіжних науковців, зокрема: В.Б. Вехов [1], В.О. Голубєв [2], В.М. Бутузов [3], Б.В. Романюк [4].

Сьогодні персональний комп'ютер, КПК, мобільний телефон з підключенням до Інтернету сприймається як належне та необхідне. Інтернет-життя щохвилини прогресує, ми поринаємо в Інтернет-магазини, форуми, онлайн-аукціони, соціальні мережі, файлообмінники та інші веб-ресурси, які займають вагоме місце в процесі життєдіяльності населення в цілому світі. Все це зумовлює збільшення популярності використання електронного грошообігу та форм розрахунку в мережі Інтернет.

Однак, нажалі, тенденція розвитку електронного грошообігу стала передумовою появи нового виду «онлайн» шахраїв, які використовуючи методи соціальної інженерії, діючи без використання шаблонних ідей, постійно вдосконалюються створюючи нові методи вчинення шахрайств відносно користувачів мережі Інтернет. Так, світова спільнота зустрілася обличчям з проблемою викрадення шахраями реквізитів банківських платіжних карток та CVV2/CVC2-кодів перевірки справжності банківської картки, за допомогою використання «фішингових веб-сайтів», Україна в цьому випадку не стала виключенням. На території України фіксуються факти створення та діяльності фішингових сайтів, які здійснюють автоматичний запис технічної інформації про номери банківських карток та CVV2/CVC2-кодів клієнтів банку, що скористались послугами «фіктивного» веб-ресурсу [5].

Фішинг (phishing) - це виманювання у потерпілих їх конфіденціальних даних методами соціальної інженерії. Як правило, мова йде про номери банківських карт, їх пінкодів, паролі до системи управління банківським рахунком (онлайн-банкінг) та іншої інформації, яку можна потім перетворити на гроші [6]. Виманювання даних відбувається за допомогою підроблених повідомлень електронної пошти або підроблених веб-сайтів. Як правило, користувача намагаються налякати, наприклад, закриттям його рахунку або припиненням надання послуг, якщо він не виконає запропоновану процедуру. Часто, якщо не завжди, посилаються на нібито в аварію, яка призвела до втрати аутентифікаційних даних, інші надзвичайні обставини, навіть на дії фішерів. Хоча ймовірність обдурити кожного адресата невелика, але за рахунок масової розсилки і охоплення величезної аудиторії фішерами вдається зібрати значну кількість цінних відомостей з кожної розсилки. Фішинг став економічно вигідний лише після появи дешевих технологій спам-розсилки [7].

Основною метою фішерів є добровільне надання користувачами інформації, а саме:

1. Номеру банківської картки.
2. Терміну дії банківської картки.
3. CVV2/CVC2-код банківської картки .

Фішинг і реалізація його є результат не однієї людини, цим займаються злочинні групи, що складаються як мінімум з двох членів. Перший спільник або група спільників займається виманюванням конфіденційних даних, які передаються або продаються другому спільникові або групі спільників для реалізації. Фішинг розрахований на людей не обізнаних в інформаційних технологіях, людей які неуважно відносяться до попереджень банків, платіжних систем та інших інстанцій. Таких - більшість.

Встановити потерпілих, які самі не звернулися до органів поліції, можливо за допомогою таких дій:

- перевірити звернення до банку чи інше підприємство, більшість обдурених не вважають за потрібне звертатися до органів поліції або думають, що сталося не шахрайство, а помилка в розрахунках, вони замість цього звертаються в банк;
- якщо є доступ до статистики трафіку або логам фішерського вебсайту, можна встановити і перевірити всіх користувачів, які зверталися до цього сайту (звичайно, не всі з них стали жертвами шахрайства, але значна частина);
- за допомогою клієнтської служби банку або самостійно розіслати всім клієнтам банку повідомлення про що мали місце спроби шахрайства з проханням перевірити свої рахунки і з обіцянкою повернути вкрадені гроші. Банк або платіжна система також можуть виступати в якості потерпілих у справі про фішинг. Можуть, але не завжди бажають, оскільки такий процес негативно позначається на діловій репутації. Однак вони завжди зацікавлені в запобіганні подальших шахрайських дій проти своїх клієнтів. Багато банків і платіжні системи самі займаються відстеженням діяльності фішперів або доручають це спеціальним агентствам [8].

Отже, розвиток сучасних інформаційних технологій має тенденції до все більшого прискорення, тому щоб не стати жертвою фішперів, варто розсудливо користуватися Інтернет-ресурсами, під час здійснення платіжних операцій, а також дотримуватись таких правил:

1. перевірити чи встановлено безпечне з'єднання по протоколу https;
2. перевірити чи веб-сайт зареєстрований на домені «ua». Наприклад за допомогою «https://2ip.com.ua» чи іншого веб-сервісу;
3. перевірити місце розташування веб-серверу, на якому розташований сайт;
4. перевірити наявність граматичних та орфографічних помилок у текстах прикріплених на сайті;
5. перевірити репутацію сайту в пошукових системах;
6. бути уважним у прийнятті рішення про користування раніше не знайомим сайтом. Користуся здоровим глуздом та логічним мисленням на противагу казковим обіцянкам та нереальним бонусним пропозиціям написаними веб-архітектором на сторінках шахрайського Інтернет ресурсу;
7. встановити антивірусне програмне забезпечення на своєму комп'ютері. Здійснити оновлення антивірусу перед кожним запуском Інтернет-браузера;
8. підключити «SMS-банкінг» та відслідковуйте всі операції, встановити щоденний ліміт по картковому рахунку в тому числі і для проведення оплат в мережі Інтернет;
9. якщо Ви часто проводите оплати або перерахування в мережі-Інтернет, то зверніться до банківської установи з метою отримання електронної (онлайн) картки, на яку ви зможете з основного рахунку перевести кошти необхідні для разової Інтернет транзакції, чим збережете інші кошти на рахунку;
10. в разі отримання SMS-повідомлення про зняття з карткового рахунку коштів, які ви не знімали або проведенню операцій по оплаті, яку ви не здійснювали необхідно негайно зателефонувати до КОЛ-центру банківської установи з метою блокування картки та звернутися до територіального управління (відділу) Департаменту кіберполіції Національної поліції України з письмовим зверненням.