4. Новик І. В. Менеджмент безпеки як невід'ємний складник інтегрованої системи менеджменту підприємства. URL: http://www.marketinfr.od.ua/journals/2019/30_2019_ukr/31.pdf

Ключові слова: менеджмент, безпека, кіберзагроза, ризики.
Key words: management, security, cyber threat, risks.

ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор фізико-математичних наук, доктор юридичних наук, професор

СЛАТВІНСЬКА ВАЛЕРІЯ МИКОЛАЇВНА

Міжнародний гуманітарний університет, викладач кафедри кримінального права, процесу та криміналістики

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗБРОЯ ХАКІНГУ З ПІДВИЩЕНИМ РИЗИКОМ

Соціальна інженерія досліджує причини поведінки людини, обставин і середовища, що впливають на формування системи її цінностей та на саму поведінку [1]. Звісно, що поведінка людей в воєнному стані або під час війни відрізняється від їх поведінки у мирний час. При цьому важливою стає створена самою людиною небезпечна (безпечна) ситуація, що проявляється, в першу чергу, в ризиках, пов'язаних з діяльністю людей. Відбувається проникнення ризику в усі сфери людської діяльності, що стає закономірним під час війни. В цьому випадку ризики реально пов'язані з несприятливими умовами життєдіяльності та небезпечними подіями та явищами (форс-мажором), що створюють небезпечні (катастрофічні) ситуації, що реалізуються. В зазначених вище умовах виникає ситуація реальної невизначеності, яка представляє собою сукупність обставин та умов, за яких можливі зміни стану об'єкта ризику стають абсолютно непередбачуваними. Ця ситуація виключає можливість об'єктивного оцінювання ризику. Однак певне зменшення невизначеності до рівня так званої статистичної невизначеності породжує ризикову ситуацію (РС), яка характеризується, існуванням кількох можливих станів (як варіант – множини станів, що сягає нескінченості), ймовірність реалізації кожного з яких відома, але в цілому невизначеність все ж таки залишається. Якщо реалізацію на об'єкт ризику будь-якого з можливих станів вважати подією, РС визначається існуванням множини варіантів можливого розвитку подій, ймовірність кожного з яких характеризується відповідною кількісною або якісною оцінкою. За умов виникнення ризикової ситуації стає актуальним проведення

аналізу й оцінювання ризиків, зокрема дослідження обставин появи, умов та форм розвинення ризиків.

В цьому екстремальному випадку під невизначеністю слід розуміти неповне або неточне уявлення про значення різних параметрів в майбутньому, що породжується неповнотою і (або) неточністю інформації щодо виникнення в ході реалізації рішення несприятливих ситуацій і наслідків, що призводить до ризику. У той же час ситуація ризику вважається фактично різновидом невизначеності, коли при настанні подій ймовірно і об'єктивно існує можливість оцінити їх вірогідність. Різниця між ризиком і невизначеністю відноситься до способу завдання інформації та визначається наявністю (у разі ризику) або відсутністю (при невизначеності) імовірнісних характеристик неконтрольованих змінних.

Достатньо швидко технічні системи захисту все більше й більше удосконалюються за рахунок постійного розвитку сучасних технологій, обліку безлічі потреб, які створюють додаткові ризики. Ще швидше це відбувається під час війи, коли люди залишаються найбільш вразливою ланкою, маючи при цьому доступ до інформації, і коли на них можна впливати методами соціальної інженерії, яка стає мистецтвом злому людської свідомості, більш підвищеної у зв'язку з підвищенням ролі соціальних мереж, електронної пошти чи інших видів он-лайн комунікації. Соціальний інжиніринг можна характеризувати як напрямок в хакінгу. Фактично це злом комп'ютерних систем, що здійснюється не тільки технічними методами, а й на рівні психології. Тоді хакінг – це фактично мистецтво експлойту. Варто відзначити, що хакінг є першочерговим елементом оскільки спочатку набувались навички кодування та виявлення вразливостей, а вже потім з'ясувалося, що за допомогою цих знань можливо отримувати користь. Саме тому з'явився напрямок психологічних прийомів введення користувачів в оману. У сфері інформаційної безпеки цей термін широко використовується для позначення ряду технік, які використовуються кіберзлочинцями. Останні мають на меті виманювання конфіденційної інформації у жертв чи спонукають жертв до здійснення дій, спрямованих на проникнення в систему обхід системи безпеки. Навіть, коли існує величезна кількість продуктів для забезпечення інформаційної безпеки, людина все ще володіє ключами від усіх дверей. Будь то комбінація облікових даних (логін та пароль), номер кредитної картки або дані для доступу до он-лайн банку, найслабша ланка в системі забезпечення безпеки – це не технології, а живі люди.

З огляду на воєнний період більшість послуг наразі доступні в онлайн і тому шанси потрапити «на гачок» врази більше. Здавалося б підібрав надійний пароль, увімкнув двофакторну ідентифікацію і ніби в безпеці. Але чи це так? Все ще є низка інтернет магазинів, які не потребують підтвердження від реальних користувачів. На просторах інтернету є купа злитих номерів банківських карток і з кожним днем база даних оновлюється. Тому буває досить несподівано отримати повідомлення про списання коштів. Скарга до банку в цьому випадку

не стане в нагоді оскільки тема безпеки онлайн покупок є й досі слабким місцем у безпеці.

В умовах воєнного стану активізується питання належного дотримання конфіденційності біометричної інформації. Наприклад, компанія Google сплачуватиме 100 млн. доларів за порушення недоторканності приватного життя користувачів.

Таким чином, якщо зловмисники застосовують до користувачів маніпулятивні психологічні техніки, дуже важливо знати, які прийоми найбільш характерні в даній ситуації, а також розуміти принцип їхньої роботи, щоб уникнути неприємностей.

Список використаних джерел:

1. Резник Ю. М. Социальная инженерия: предметная область и границы применения. Социс. 1994. № 2. С. 28–34.

Ключові слова: соціальна інженерія, людина, ризики, інформаційні ризики, невизначеність, хакинг.
Key words: social engineering, people, risks, information risks, invisibility, hacking.

СТРЕЛКОВСЬКА ІРИНА ВІКТОРІВНА

Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор

СОЛОВСЬКА ІРИНА МИКОЛАЇВНА

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

ПРОГНОЗУВАННЯ МУЛЬТИМЕДІЙНОГО ТРАФІКУ ПРИСТРОЇВ ІНТЕРНЕТ РЕЧЕЙ IOT/5G

Динамічний розвиток послуг Інтернет речей IoT (Internet of Things) для мереж п’ятого покоління 5G відбувається в межах груп, класифікованих згідно [1; 2]: надширокосмуговий мобільний зв’язок eMBB (enhanced Mobile Broadband), масовий міжмашинний зв’язкок mMTC (massive Machine-Type Communications) та наднадійний машинний зв’язок з низькими затримками URLLC (Ultra-Reliable Low Latency Communication), включаючи послуги тактильного Інтернет та голографічні послуги. Впровадження таких послуг вимагатиме від IoT пристроїв значного збільшення швидкості передачі даних та забезпечення значень характеристик якості обслуговування та сприйняття QoS/QoE (Quality of Service/Experience) [1; 2]. Особливу увагу, з погляду реалізації послуг IoT, слід приділити активному використанню мультимедійних