УДК: 338.262.8

Бойко А.Б.

ІНФОРМАЦІЙНІ ЗАГРОЗИ ДЛЯ ОПЕРАТОРІВ МОБІЛЬНОГО ЗВ'ЯЗКУ

Постановка проблеми. Для успішної діяльності усіх компаній, що надають послуги мобільного зв'язку, інформаційна безпека (ІБ) є складовим і невід'ємним елементом бізнесу, яка в наш час стала частиною загальної системи управління в організації, що відноситься до даних видів діяльності. При грамотній організації система інформаційної безпеки може реалізуватися в конкурентну перевагу, підвищити інвестиційну привабливість компанії, налагодити бізнес-процеси і поліпшити імідж оператора.

Мета дослідження полягає у визначенні і попередженні найпоширеніших загроз, які можуть спіткати більшість компаній з надання послуг мобільного зв'язку.

Огляд останніх досліджень і публікацій. Авторами найвизначніших праць, що склали методологічну основу досліджень інформаційного суспільства, є Д. Белл, М. Кастельс та інші. У своїх роботах вони дали визначення інформаційного суспільства, окреслили його основні риси, позитивні та негативні наслідки розвитку [4,5].

В Україні вивчення цих питань розпочалося в 90-х рр. минулого століття. Такі вчені, як Г. Почепцов, О. Морозов, В. Королько та інші, приділяють увагу вивченню особливостей становлення інформаційного суспільства в українських реаліях [1,2,3].

Виклад основного матеріалу. Говорячи «телеком», фахівцеві в області ІБ відразу представляється два «образи»: «образ» об'єкта захисту і «образ» порушника. Під об'єктами захисту ми розуміємо інформацію і ключові бізнес-процеси.

Спробуємо ж перерахувати компоненти «образу» об'єкта захисту для операторів мобільного зв'язку:

1. Інформація:

- таємниця зв'язку - відомості про передані по мережах зв'язку повідомлення;
- відомості про абонентів (юридичних і фізичних осіб)
- комерційна таємниця (в тому числі плани розвитку послуг, тарифікації і т.п.);
- персональні дані працівників.

2. Білінг - процеси тарифікації, виставлення рахунків, обробки платежів і т.п.

3. Інформаційні системи

- білінгова система - інформаційна інфраструктура, що включає системи обробки та аналізу інформації, технічні і програмні засоби її обробки, передачі та відображення, в тому числі канали інформаційного обміну і телекомунікації, системи і засоби захисту інформації, об'єкти і приміщення, в яких розміщені компоненти білінгової системи);
- інформаційні системи персональних даних оператора.

«Образ» потенційного порушника було б логічно описати з точки зору його відношення до інфраструктури компанії і його прав на доступ до об'єкта захисту. Цілком очевидно, що перший розподіл буде на зовнішніх і внутрішніх порушників. Внутрішні порушники мають санкціонований доступ до інформації, що захищається, а зовнішні порушники не мають такого доступу, відповідно їх методи і сценарії реалізації загроз будуть різнитися. Другий розподіл проводиться щодо місця, з якого діє порушник.

Так, найбільшими «привілеями» будуть володіти особи, які мають доступ безпосередньо до технологічної інфраструктури - це адміністратори систем і мереж, працівники компанії, деякі партнери, яким надано доступ в технологічну мережу, для надання необхідних послуг.

Що ще потрібно враховувати при оцінці ризиків інформаційної безпеки для операторів? Перш за все те, що компанія по наданню послуг мобільного зв'язку - це:

- величезні мережі;

- територіальна розподіленість;
- поєднання різних послуг в рамках єдиної складної інфраструктури;
- величезна кількість додатків і систем на об'єктах, які часто мають різні ступені критичності і відповідні їм вимоги з безпеки.

Найбільш істотні ризики для операторів виглядають наступним чином:

- відтік клієнтів;
- зниження репутації (імідж), як наслідок - відтік клієнтів, упущена вигода;
- втрата конкурентних переваг;
- фінансові витрати на усунення наслідків;
- невідповідність законодавству, вимогам регулюючих органів (аж до відкликання ліцензії).

Візьмемо топ-3 кожного виду загроз. Вони представлені в порядку їх значущості (табл. 1, 2, 3). Для їх розподілу нами використано результати, які отримала компанія LETA у своїй аналітичній роботі «Інформаційна безпека. Огляд ризиків. Телеком» [6].

Таблиця 1

Загрози, пов'язані з будь-якими видами шахрайства у сфері зв'язку:

Загроза	**Актив, на який спрямована загроза**	**Ризики реалізації загроз**	**Контрзаходи по нейтралізації загроз**
Шахрайство, спрямоване на розкрадання коштів абонентів	Білінг	Відтік клієнтів; зниження репутації	Використання систем аналізу відхилень у поведінці абонентів з метою виявлення дій, характерних для зловмисників (FMS - Fraud Management System); постійний моніторинг використовуваних зловмисниками схем і вироблення індивідуальних підходів до максимальної нейтралізації відповідної вразливості
Шахрайство, спрямоване на розкрадання коштів оператора (за рахунок системи взаєморозрахунків між операторами)	Білінг	Фінансові витрати	Використання систем аналізу відхилень у поведінці абонентів з метою виявлення дій, характерних для зловмисників (FMS); постійний моніторинг використовуваних зловмисниками схем і вироблення індивідуальних підходів до максимальної нейтралізації відповідної вразливості

Таблиця 2

Загрози, пов'язані з навмисними діями (вмисною дезорганізацією роботи, виведення з ладу і т.п.), і заходи щодо їх нейтралізації та зниження можливого збитку:

Загроза	Актив, на який спрямована загроза	Ризики реалізації загроз	Контрзаходи по нейтралізації загроз
Фізичне руйнування або виведення з ладу всіх або окремих найбільш важливих компонентів автоматизованої системи (пристроїв, носіїв важливої системної інформації), відключення або вивід з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, ліній зв'язку і т.п.	Білінгова система	Відтік клієнтів; зниження репутації	Організаційні заходи (регламентація дій, введення заборон); застосування фізичних засобів, що перешкоджають навмисного скоєння порушення; резервування критичних ресурсів
Впровадження агентів у число персоналу системи (у тому числі, можливо, і в адміністративну групу, яка відповідала за безпеку), вербування (шляхом підкупу, шантажу, погроз і т.п.) користувачів, що мають певні повноваження по доступу до ресурсів, що захищаються	Таємниця зв'язку; відомості про абонентах; комерційна таємниця; персональні дані працівників; білінгва система (якщо метою впровадження є порушення її роботоспро-можності)	Втрата конкурентних переваг; відтік клієнтів	Організаційні заходи (підбір, розстановка і робота з кадрами, посилення контролю та відповідальності); автоматична реєстрація дій персоналу; організаційні і технічні заходи по застосуванню систем захисту персональних комп'ютерів (в частині виявлення і блокування програм-агентів)
Розкрадання носіїв інформації (роздруківок, магнітних дисків, стрічок, запам'ятовуючих пристроїв і цілих ПВЕМ), розкрадання виробничих відходів (роздруківок записів, списаних носіїв інформації тощо)	Таємниця зв'язку; відомості про абонентів; комерційна таємниця; персональні дані працівників	Втрата конкурент - них переваг; зниження репутації; накладення штрафних санкцій регулятором аж до відкликання ліцензії	Організаційні заходи (організація зберігання та використання носіїв з захищається інформацією, регламентація робіт з зазначеними захищеними носіями)

Як видно, загрозами можуть бути, як шахрайство, так і виведення з ладу обладнання, або, як шпигунство, так і ненавмисні дії працівників компаній. Це все може призвести до зниження репутації компанії, втраті конкурентних переваг, відтоку клієнтів, і, як правило, значних фінансових витрат, що спричинить втрату частини прибутку, а державою – втрати частини надходження в бюджет від податку на прибуток підприємства мобільного зв’язку.

Таблиця 3

Загрози, пов'язані з ненавмисними діями, і заходи щодо їх нейтралізації та зниження можливого збитку

Загроза	Актив, на який спрямова на загроза	Ризики реалізації загроз	Контрзаходи по нейтралізації загроз
Дії працівників, що призводять до часткового або повної відмови системи або порушення працездатності апаратних чи програмних засобів, відключенню обладнання або зміні режимів роботи пристроїв та програм, руйнування інформаційних ресурсів системи (ненавмисне псування устаткування, видалення, спотворення програм або файлів з важливою інформацією, в тому числі системних файлів, пошкодження каналів зв'язку, навмисне псування носіїв інформації тощо)	Білінгова система	Фінансові витрати на усунення наслідків; відтік клієнтів; зниження репутації	Організаційні заходи (регламентація дій, введення заборон); застосування фізичних засобів, перешкодження навмисному скоєнню порушення; резервування критичних ресурсів
Несанкціонований запуск технологічних програм, здатних при некомпетентному використанні, викликати втрату працездатності системи (зависання та зациклення) або здійснення незворотних змін в системі (форматування або реструктуризацію носіїв інформації, видалення даних)	Білінгова система	Фінансові витрати на усунення наслідків	Організаційні заходи (видалення всіх потенційно небезпечних програм з дисків робочих станцій); застосування технічних (апартно-програмних) засобів розмежування доступу до технологічних і інструментальних програм на дисках робочих станцій
Несанкціоноване впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та інших, які не є необхідними для виконання співробітниками своїх службових обов'язків) з подальшим необгрунтованим витрачанням ресурсів (процесорного часу, оперативної пам'яті, пам'яті на зовнішніх носіях і т.п	Білінгова система	Фінансові витрати на усунення наслідків	Організаційні заходи (введення обмежень). Контроль налаштувань робочих станцій; застосування технічних (апартно-програмних) засобів і налаштувань, що перешкоджають несанкціонованому впровадження та використання неврахованих програм

Висновки. Так, як розвиток телекомунікаційного ринку відбувається з величезною швидкістю - це і багаточисельні приклади поглинань, і поява нових технологій, і постійно мінлива інфраструктура, все це, природно, породжує нові загрози, види атак і хитрощів зловмисників. І як наслідок, вимагає непростих рішень і матеріальних затрат для фахівців з інформаційної безпеки, компаній з надання послуг мобільного зв'язку, на чиї плечі лягають турботи про проектування безпечних систем і підтримка їх на необхідному рівні захисту. Звичайно, краще попереджувати такі небезпеки, ніж нести фінансові витрати на усунення наслідків, мати відтік клієнтів та зниження репутації.

Анотація

Досліджено типи інформаційних загроз та окреслено шляхи їх попередження та нейтралізації.

Ключові слова: інформаційна загроза, білінг, інформаційна безпека, об'єкт захисту, порушник.

Анотация

Исследованы типы информационных угроз и намечены пути их предупреждения и нейтрализации.

Ключевые слова: информационная угроза, биллинг, информационная безопасность, объект защиты, нарушитель.

Summary

A study of the types of information threats and methods of their prevention.

Keywords: security threat, billing, information security, object of protection, intruder.

Список використаних джерел:

1. Почепцов Г.Г. Информационные войны. Основы военно-коммуникативных исследований. – Киев, 1998.
2. Морозов О. Інформаційна безпека в умовах сучасного стану і перспективи розвитку державності // Віче. – 2007. – № 12. – Спецвипуск. – С. 23
3. Основні принципи побудови інформаційних кампаній в контексті тематики „ВІЛ та діти". Посібник для організаторів. / За редакцією доктора філософських наук Королька В.Г. К., 2006. – 68 с.
4. Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. — Москва: Прогресс, 1986. — с. 330—342
5. Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О. И. Шкаратана. — М.: ГУ ВШЭ, 2000. — 608 с.
6. Офіційний сайт. [Електронний ресурс]. – Доступний з http://www.letagroup.ru/rus/library/research.html