13. Відомості про зареєстровані вУкраїні кваліфіковані зазначення походження товарів [Електронний ресурс] // Режим доступу: http://sips.gov.ua/ua/kzpt_Uk
14. Угода про асоціацію між Україною, з однієї сторони, та Європейським союзом, Європейським співтовариством з атомної енергії і їхніми державами – членами, з іншої сторони [Електронний ресурс] // Режим доступу: http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_(body).pdf
15. Додаток XXII-D Географічні зазначення вин, ароматизованих вин та алкогольних напоїв, згадані у статтях 202(3) І 202(4) цієї Угоди [Електронний ресурс] // Режим доступу: http://www.kmu.gov.ua/docs/EA/Annexes_title_IV/22_Annexes_D.pdf
16. Звіт про діяльність Харківського обласного територіального відділення Антимонопольного комітету України в 2012 році [Електронний ресурс] // Режим доступу: http://www.amc.gov.ua/amku/control/kha/uk/publish/article/80391;jsessionid=9C3F9C9158A3B36D8967F669DBE660F9
17. Андрощук Г.О. «Сендвіч-сир з пармезаном» - без пармезану!? / Г. Андрощук // Інтелектуальна власність в Україні – 2013- № 7 — С.50-54.
18. Ляшенко С. Охорона прав інтелектуальної власності, які стосуються природних мінеральних вод //Інтелектуальна власність – 2011.-№8. – С.20-27.
19. Науково-практичний коментар до Закону України «Про захист від недобросовісної конкуренції». Науково-практичне видання / Г. О. Андрощук, Т. Б. Бондарєв, Н. А. Іваницька, С. В. Шкляр. — К.: ВД «Юридична газета», 2013. — 176 с.
20. Андрощук Г. Водка "Русская": наименование места происхождения, общеизвестный знак или наименование, вошедшее во всеобщее употребление?! / Г. Андрощук // Інтелектуальна власність.- 2011- №6.- С.11-19.
21. Коваленко И. Новые географические указания в Молдове // Экономическое обозрение, № 30 (1006) 23 августа 2013 [Електронний ресурс] // Режим доступу: http://logos.press.md/node/37370
22. Економічна складова Угоди про асоціацію між Україною та ЄС: наслідки для бізнесу, населення та державного управління//Інститут економічних досліджень і політичних консультацій. – К.: 2014.—141 с. [Електронний ресурс] // Режим доступу: http://www.ier.com.ua/files//Projects/2013/EU_Ukraine/Economic_red.pdf
23. Про затвердження Положення про Перелік видових назв товарів МОН України; Наказ, Положення від 12.12.2000 № 583. [Електронний ресурс] // Режим доступу: http://zakon4.rada.gov.ua/laws/show/z0061-01/print
24. Евроловушки для Украины. ”Бурдей“ вместо ”Шампанского“ [Електронний ресурс] // Режим доступу: http://trueinform.ru/modules.php?name=News&file=print&sid=18199
25. Evaluation of the CAP policy on protected designations of origin (PDO) and protected geographical indications (PGI). London Economics, November 2008.

ГЛАВА 3.7. ОСНОВНІ ПОРУШНИКИ ТА ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

Башинська І.О.
к.е.н., старший викладач кафедри обліку, аналізу та аудиту
Одеський національний політехнічний університет

Сьогодні на автоматизованих промислових підприємствах тема інформаційної безпеки стає все більш актуальною. Сучасні системи автоматизації забезпечують високий рівень комунікації. Нові системи засновані на поширених на ринку IT-платформах, багато з яких, як відомо, уразливі до електронних атак.

Під *порушником інформаційної безпе*ки розуміється особа, яка в результаті навмисних або ненавмисних дій може завдати шкоди інформаційних ресурсів підприємства [1].

Під *атакою* на ресурси корпоративної мережі розуміється спроба нанесення шкоди інформаційних ресурсів систем, підключених до мережі. Атака може здійснюватися як безпосередньо порушником, так і опосередковано, за допомогою процесів, що виконуються від імені порушника, або шляхом впровадження в систему програмних або апаратних закладок, комп'ютерних вірусів, троянських програм і т. т.

Всі порушники за ознакою приналежності до підрозділів, що забезпечують функціонування інформаційної системи (ІС), діляться на зовнішніх і внутрішніх.

Внутрішні порушники. Внутрішнім порушником може бути особа з наступних категорій співробітників обслуговуючих підрозділів:

- обслуговуючий персонал (системні адміністратори, адміністратори БД, адміністратори додатків і т.п., що відповідають за експлуатацію і супровід технічних і програмних засобів);
- програмісти, відповідальні за розробку та супровід системного і прикладного ПЗ;
- технічний персонал (робітники підсобних приміщень, прибиральниці і т. п.);
- співробітники бізнес підрозділів підприємства, яким надано доступ в приміщення, де розташовано комп'ютерне або телекомунікаційне обладнання.

Передбачається, що несанкціонований доступ на об'єкти системи сторонніх осіб виключається заходами фізичного захисту (охорона території, організація пропускного режиму і т. П.).

Припущення про кваліфікацію внутрішнього порушника формулюються таким чином [2]:

- внутрішній порушник є висококваліфікованим фахівцем у галузі розробки та експлуатації ПЗ і технічних засобів;
- знає специфіку завдань, що вирішуються обслуговуючими підрозділами ІС підприємства;
- є системним програмістом, здатним модифікувати роботу операційних систем;
- правильно представляє функціональні особливості роботи системи і процеси, пов'язані зі зберіганням, обробкою і передачею критичної інформації;
- може використовувати як штатне обладнання і ПЗ, наявні в складі системи, так і спеціалізовані засоби, призначені для аналізу і злому комп'ютерних систем.

Залежно від способу здійснення доступу до ресурсів системи та надаються їм повноважень внутрішні порушники поділяються на п'ять категорій.

Категорія А: не зареєстровані в системі особи, які мають санкціонований доступ в приміщення з обладнанням. Особи, що відносяться до категорії А можуть: мати доступ до будь фрагментам інформації, що розповсюджується по внутрішніх каналах зв'язку корпоративної мережі; розташовувати будь-якими фрагментами інформації про топологію мережі, про використовувані комунікаційних протоколах і мережевих сервісах; розташовувати іменами зареєстрованих користувачів системи і вести розвідку паролів зареєстрованих користувачів.

Категорія В: зареєстрований користувач системи, що здійснює доступ до системи з віддаленого робочого місця. Особи, що відносяться до категорії В: своєму розпорядженні всі можливості осіб, які належать до категорії А; знають, принаймні, одне легальне ім'я доступу; володіють усіма необхідними атрибутами, що забезпечують доступ до системи (наприклад, паролем); мають санкціонований доступ до інформації, що зберігається в БД і на файлових серверах корпоративної мережі, а також на робочих місцях користувачів. Повноваження користувачів категорії В з доступу до інформаційних ресурсів корпоративної мережі підприємства повинні регламентуватися політикою безпеки, прийнятої на підприємстві.

Категорія С: зареєстрований користувач, який здійснює локальний або віддалений доступ до систем входять до складу корпоративної мережі. Особи, що відносяться до категорії С: володіють всіма можливостями осіб категорії В; мають інформацію про топології мережі, структурі БД і файлових систем серверів; мають можливість здійснення прямого фізичного доступу до технічних засобів ІС.

Категорія D: зареєстрований користувач системи з повноваженнями системного (мережевого) адміністратора. Особи, що відносяться до категорії D: володіють всіма можливостями осіб категорії С; володіють повною інформацією про системний і прикладному програмному забезпеченні ІВ; володіють повною інформацією про технічні засоби та конфігурації мережі; мають доступ до всіх технічних і програмних засобів ІС і володіють правами налаштування технічних засобів і ПЗ. Концепція безпеки вимагає

підзвітності осіб, які належать до категорії D та здійснення незалежного контролю над їх діяльністю.

Категорія E: програмісти, відповідальні за розробку та супровід загальносистемного і прикладного ПЗ, використовуваного в ІС. Особи, що відносяться до категорії E: володіють можливостями внесення помилок, програмних закладок, установки троянських програм і вірусів на серверах корпоративної мережі; можуть розташовувати будь-якими фрагментами інформації про топологію мережі і технічних засобах ІС [1].

Зовнішні порушники. До зовнішніх порушників належать особи, перебування яких в приміщеннях з обладнанням без контролю з боку співробітників підприємства неможливо.

Зовнішній порушник: здійснює перехоплення, аналіз і модифікацію інформації, переданої по лініях зв'язку, які проходять поза контрольованої території; здійснює перехоплення і аналіз електромагнітних випромінювань від устаткування ІС.

Припущення про кваліфікацію зовнішнього порушника формулюються таким чином:

- є висококваліфікованим фахівцем у галузі використання технічних засобів перехоплення інформації;
- знає особливості системного і прикладного ПЗ, а також технічних засобів ІС;
- знає специфіку завдань, що вирішуються ІС;
- знає функціональні особливості роботи системи та закономірності зберігання, обробки і передачі в ній інформації;
- знає мережеве та канальне обладнання, а також протоколи передачі даних, що використовуються в системі;
- може використовувати тільки серійно виготовляється спеціальне обладнання, призначене для знімання інформації з кабельних ліній зв'язку та з радіоканалів.

При використанні моделі порушника для аналізу можливих загроз ІБ необхідно враховувати можливість змови між внутрішніми і зовнішніми порушниками.

Захист інформаційних компонентів і групи загроз. В якості об'єктів захисту виступають наступні види інформаційних ресурсів підприємства:

- інформація (дані, телефонні переговори і факси) передана каналами зв'язку.
- інформація, збережена в базах даних, на файлових серверах і робочих станціях, на серверах каталогів, у поштових скриньках користувачів корпоративної мережі і т.п.
- конфігураційна інформація та протоколи роботи мережевих пристроїв, програмних систем і комплексів [3].

Виходячи з перерахованих властивостей, всі загрози інформаційних ресурсів системи можна віднести до однієї з наступних категорій:

- загрози доступності інформації, що зберігається і оброблюваної в ІС та інформації, що передається каналами зв'язку;
- загрози цілісності інформації, що зберігається і оброблюваної в ІС та інформації, що передається каналами зв'язку;
- загрози конфіденційності інформації зберігається і оброблюваної в ІС та інформації, переданої по каналах зв'язку.

Загрози безпеці інформаційних ресурсів, *з точки зору реалізації*, можна розділити на наступні групи:

1. Загрози, що реалізуються з використанням технічних засобів;
2. Загрози, що реалізуються з використанням програмних засобів;
3. Загрози, що реалізуються шляхом використання технічних каналів витоку інформації.

1. Загрози, що реалізуються з використанням технічних засобів. Технічні засоби системи включають в себе приймально-передавальний і комутуюче обладнання, обладнання серверів і робочих станцій, а також лінії зв'язку. До даного класу відносяться загрози доступності, цілісності і, в деяких випадках конфіденційності інформації, що зберігається, обробляється і передається по каналах зв'язку системи, пов'язані з ушкодженнями та

відмовами технічних засобів ІС, приймально-передавального і комутуючого обладнання та пошкодженням ліній зв'язку.

Для технічних засобів характерні загрози, пов'язані з їх умисним або ненавмисним пошкодженням, помилками конфігурації і виходом з ладу:

- виведення з ладу (умисний чи ненавмисний);
- несанкціоноване або помилкове зміна конфігурації активного мережного обладнання та приймально-передавального обладнання;
- фізичне пошкодження технічних засобів, ліній зв'язку, мережевого і каналоутвоюючого обладнання;
- перебої в системі електроживлення;
- відмови технічних засобів;
- установка неперевірених технічних засобів або заміна що вийшли з ладу апаратних компонент на неідентичні компоненти;
- розкрадання технічних засобів і довготривалих носіїв конфіденційної інформації внаслідок відсутності контролю над їх використанням та зберіганням.

В якості джерел загроз безпеці для технічних засобів системи виступають як зовнішні і внутрішні порушники, так і природні явища. Серед джерел загроз для технічних засобів можна відзначити:

- стихійні лиха;
- пожежа;
- крадіжка обладнання;
- саботаж;
- помилки обслуговуючого персоналу;
- тероризм і т. п.

2. Загрози, що реалізуються з використанням програмних засобів. Це найбільш численний клас загроз конфіденційності, цілісності та доступності інформаційних ресурсів, пов'язаний з отриманням несанкціонованого доступу до інформації, що зберігається і оброблюваної в системі, а також передається по каналах зв'язку, за допомогою використання можливостей, що надаються ПО ІВ. Більшість розглянутих в цьому класі загроз реалізується шляхом здійснення локальних або віддалених атак на інформаційні ресурси системи внутрішніми і зовнішніми зловмисниками. Результатом успішного здійснення цих загроз стає отримання несанкціонованого доступу до інформації БД і файлових систем корпоративної мережі, даних, що зберігаються на АРМ операторів, конфігурації маршрутизаторів та іншого активного мережного обладнання.

У цьому класі розглядаються такі основні види загроз:

- впровадження вірусів і інших руйнуючих програмних дій;
- порушення цілісності виконуваних файлів;
- помилки коду і конфігурації ПО, активного мережевого обладнання;
- аналіз і модифікація ПЗ;
- наявність в ПО декларованих можливостей, залишених для налагодження, або зумисне впроваджених;
- спостереження за роботою системи шляхом використання програмних засобів аналізу мережевого трафіку і утиліт ОС, що дозволяють отримувати інформацію про систему і про стан мережних з'єднань;
- використання вразливостей ПЗ для злому програмного захисту з метою отримання несанкціонованого доступу до інформаційних ресурсів або порушення їх доступності;
- виконання одним користувачем несанкціонованих дій від імені іншого користувача («маскарад»);
- розкриття, перехоплення і розкрадання секретних кодів і паролів;
- читання залишкової інформації в ОП комп'ютерів і на зовнішніх носіях;
- помилки введення керуючої інформації з АРМ операторів в БД;

– завантаження та встановлення в системі не ліцензійного, неперевіреного системного і прикладного ПЗ;

– блокування роботи користувачів системи програмними засобами.

Окремо слід розглянути загрози, пов'язані з використанням мереж передачі даних. Даний клас загроз характеризується отриманням внутрішнім або зовнішнім порушником мережевого доступу до серверів БД і файлових серверів, маршрутизаторів і активного мережевого обладнання. Тут виділяються наступні види загроз, характерні для КСПД підприємства:

– перехоплення інформації на лініях зв'язку шляхом використання різних видів аналізаторів мережевого трафіку;

– заміна, вставка, видалення або зміна даних користувачів в інформаційному потоці;

– перехоплення інформації (наприклад, користувача паролів), переданої по каналах зв'язку, з метою її подальшого використання для обходу засобів мережевої аутентифікації;

– статистичний аналіз мережевого трафіку (наприклад, наявність або відсутність певної інформації, частота передачі, напрям, типи даних і т. п.).

В якості джерел загроз безпеці для технічних засобів системи виступають як зовнішні і внутрішні порушники.

3. Загрози витоку інформації технічними каналами зв'язку. Види технічних каналів витоку інформації.

При проведенні робіт з використанням конфіденційної інформації та експлуатації технічних засобів ІС можливі наступні канали витоку або порушення цілісності інформації або працездатності технічних засобів:

– побічні електромагнітні випромінювання інформативного сигналу від технічних засобів і ліній передачі інформації;

– акустичне випромінювання інформативного мовного сигналу або сигналу, обумовленого функціонуванням технічних засобів обробки інформації;

– несанкціонований доступ до інформації, що обробляється в автоматизованих системах;

– розкрадання технічних засобів з зберігається в них інформацією або окремих носіїв інформації;

– перегляд інформації з екранів дисплеїв і інших засобів її відображення за допомогою оптичних засобів;

– вплив на технічні чи програмні засоби з метою порушення цілісності (знищення, спотворення) інформації, працездатності технічних засобів.

Найбільшу небезпеку в даний час для промислових підприємств представляють технічні засоби розвідки:

– акустична розвідка;

– розвідка побічних електромагнітних випромінювань і наведень електронних засобів обробки інформації (далі - ПЕМВН);

– в окремих ситуаціях, можуть використовуватися: телевізійна, фотографічна і візуальна оптична розвідка, що забезпечує добування інформації, що міститься в зображеннях об'єктів, одержуваних у видимому діапазоні електромагнітних хвиль з використанням телевізійної апаратури.

Крім перехоплення інформації технічними засобами розвідки можливо ненавмисне влучення конфіденційної інформації до осіб, які не допущеним до неї, але знаходяться в межах контрольованої зони. Витік інформації можлива за такими каналами:

– радіоканали;

– ІЧ-канал;

– ультразвуковий канал;

– дротові лінії.

В якості провідних ліній при передачі інформації до зовнішніх засобам реєстрації можуть бути використані:

– мережі змінного струму;
– лінії телефонного зв'язку;
– радіотрансляційні й технологічні (пожежної, охоронної сигналізації, кабелі телеантен і т.п.) лінії;
– спеціально прокладені провідні лінії.

При застосуванні лазерної апаратури дистанційного прослуховування, що фіксує інформативні коливання скла у вікнах приміщень, можливий з'їм акустичної інформації з виділених приміщень, в яких встановлені елементи системи.

В якості джерел загроз безпеці для технічних засобів системи виступають як зовнішні і внутрішні порушники, оснащені спеціалізованими засобами технічної розвідки.

Таким чином, концепція захисту інформаційної безпеки промислового підприємства повинна бути призначена для вирішення наступних завдань:

– захисту зовнішнього периметра корпоративної мережі підприємства від загроз з боку зовнішніх мереж за рахунок використання міжмережевого екранування, контролю віддаленого доступу та моніторингу інформаційних взаємодій.
– захисту корпоративних серверів за рахунок використання механізмів управління доступом до серверів баз даних, файловим, інформаційним і поштових серверів, реєстрації та обліку подій, пов'язаних із здійсненням доступу до ресурсів корпоративних серверів, механізмів моніторингу та аудиту безпеки.
– комплексного антивірусного захисту систем, що входять до складу корпоративної мережі за рахунок розподілу антивірусних засобів (антивірусних сканерів, резидентних антивірусних моніторів і файлових ревізорів.

Література:

1. Н. Леффлер, П. Тервиш: Аспекты производительности, АББ Ревю №2/2004.
2. M. Naedele: IT Security for Automation Systems – Motivations and Mechanisms, atp international, Vol 1 (1), 11/2003, and atp, Vol 45 (5), 5/2003
3. Башинська І.О. Інформаційна безпека комерційної таємниці промислових підприємств // Съвременни проблеми на регионалното развитие: Събрани статии. Т. 2. – Академично издателство на Аграрния университет Пловдив, България, 2014. – 368 с. – С. 174-176 http://conf.at.ua/27-28.10.2014_Vol.2.pdf

ГЛАВА 3.8. РИЗИКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ В КРЕДИТНІЙ СФЕРІ

Бондаренко Л.А.

кандидат економічних наук, доцент

ДВНЗ «Криворізький національний університет» Криворізький економічний інститут

Проведення кредитних операцій є одним з головних джерел ризику для банку, оскільки кредити складають істотну частину банківських активів. Правильне визначення поняття кредитного ризику має першочергове значення для його виміру, прогнозування і вирішення інших задач, пов’язаних з формуванням системи управління банку.

В результаті дослідження точок зору про сутність кредитного ризику, які існують в економічній літературі, автором виявлено три підходи (табл. 1).

Зміст кредитного ризику частіше за все розкривається з погляду джерела виникнення і форми прояву. Більшість авторів визначає кредитний ризик як вірогідність втрати частини активів банку, які формують кредитний портфель.

Дослідники іншого напряму трактують кредитний ризик як можливе зменшення прибутку банку або небезпеку зазнати збитки внаслідок невиконання умов договору.

Вважаємо, що більш ємко розглядають кредитний ризик дослідники третього напряму. Вони не обмежують поняття кредитного ризику лише вірогідністю втрати частини активів, зменшенням прибутку чи отриманням збитку. Головною характеристикою кредитного ризику, на їх думку, є порушення умов кредитної угоди, незалежно від наслідків для банку.