2. THE INSTITUTIONAL FOUNDATIONS OF INDUSTRY'S ECONOMIC DEVELOPMENT

ГЛАВА 2.1. СУЧАСНІ ТЕНДЕНЦІЇ НА РИНКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Башинська І.О.
канд. екон. наук, старший викладач кафедри обліку, аналізу та аудиту
Одеський національний політехнічний університет

На сьогоднішній день інформаційна сфера є ведучою в діяльності держави і чинить вплив на всі елементи функціонування промислових підприємств. Разом зі зростаючою залежністю від електронних технологій, пов'язаних з поширенням інформації, зростає і загроза кібератак, метою, яких, як правило, стають інформаційні ресурси та мережева інфраструктура [1].

В організації ефективної комплексної системи безпеки не останнє місце займає її інформаційна підсистема, метою якої є формування достатньої сукупності матеріалів і відомостей щодо середовища функціонування установи або організації та їх якісна аналітична обробка і захист від пошкодження, викрадення, деформації, втрати з метою отримання достовірних даних, необхідних для прийняття ефективних управлінських рішень.

Головна задача інформаційної безпеки (кінцевий результат) полягає у вирішенні інформаційно-аналітичними засобами не тільки проблем захисту від загроз, що виникають, а, перш за все, завчасне розкриття і попередження суб'єкта управління про причини і умови, які можуть сприяти виникненню ранніх ознак цих загроз , а саме: ризиків, небезпек і викликів [3].

Під *економічною безпекою* розуміють власне стан економічної системи, що характеризується наявністю конкурентних переваг, які досягаються ефективним використанням існуючих власних та залучених ресурсів, своєчасним впровадженням комплексу заходів з метою підтримання нормальних умов працездатності системи для максимального досягнення поставлених цілей у короткостроковому та довгостроковому періоді в умовах постійної зміни навколишнього середовища [2].

Сучасні тенденції на ринку інформаційно-аналітичного забезпечення економічної безпеки підприємства базуються на комплексному підході, а саме захисту підприємства з таких боків:

1) захист від вторгнень;
2) захист від витоків інформації;
3) захист файлів і документів;
4) забезпечення відмовостійкості і безперервності бізнес-процесів;

Розглянемо сучасні тенденції для захисту кожної складової:

1. Для боротьби з вторгненнями використовується два типи систем: системи запобігання вторгнень (IPS) та системи виявлення вторгнень (IDS). Їхні переваги та недоліки наочно представлені у табл. 1.

Система визначає вторгнення двома основними методами:

Сигнатурний аналіз – система звіряє активність мережі з базою відомих вторгнень (сигнатур), які постійно оновлюються, і сигналізує про вторгнення при збігу активності з даними еталоном.

Визначення аномалій – система аналізує нормальний стан мережі і запам'ятовує його як еталон. У випадках значного відхилення від нього поточної мережевої активності, система визначає це як аномалію і сигналізує про це.

Сучасні системи захисту від вторгнень не є поодинокими рішеннями, а представляють із себе комплекс, що об'єднує функції роутера, файєрвола і IDS / IPS.

Таблиця 1

Порівняння систем захисту від вторгнень

Параметри / Системи захисту	Системи запобігання вторгнень (IPS)	Системи виявлення вторгнень (IDS).
Основні відмінності	Застосовуються для блокування підозрілої мережевої активності і відсівають нелегітимний трафік.	Відслідковують аномалії в мережі і сигналізують про можливе вторгнення адміністратору.
Переваги	Дозволяє не тільки виявити, але й запобігти вторгненню.	Дозволяє боротися з вторгненнями і в той же час не заважає роботі користувачів. Рішення про запобігання атаки приймає адміністратор.
Недоліки	Велика кількість помилкових спрацьовувань, які знижують продуктивність праці співробітників компанії і можуть призводити до простоїв IT-інфраструктури.	Існує ризик, що адміністратор не встигне вжити заходів щодо запобігання вторгнення і компанія встигне понести збитки.

2. Захист від витоків інформації – це комплекс заходів, спрямований на забезпечення збереження і цілісності інформації. Під інформацією в даному випадку мається на увазі інформація компанії, яка використовується в зовнішньому і внутрішньому документообігу. Така інформація зберігається у вигляді набору документів, що не підлягають зміні без рішення керівництва компанії, і називається конфіденційною. Основні проблеми та сучасні засоби їх вирішення представлені у табл. 2.

Таблиця 2

Основні проблеми витоку інформації та варіанти їх вирішення

Проблема	Рішення
Витік документів компанії від співробітників, інсайдерів.	**Symantec DLP** – захищає, попереджає, запобігає (в залежності від настройки) витоку конфіденційних даних, шляхом перевірки листів, месенджерів, веб-трафіку користувачів. **Right Management Services** – при витоку інформації, не дає доступ користувачеві до даних. Тобто якщо користувач зміг винести документ, то це ще не означає що він відкриє його на іншому комп'ютері без відповідних прав. **SafeNet DataSecure** – комплексне рішення спрямоване на забезпечення безпеки на всьому періоді її існування. В сценарії використання цієї системи - всі дані компанії зашифровані. Шифрування відбувається прозоро для користувачів і бізнес-процесів, не знижуючи продуктивності існуючих платформ. Дані зашифровані на всіх рівнях - на рівні бази даних, додатків, диска, папки або файлу. Система сама вводить ваш секретний ключ для розшифровки документів, і веде журнали доступу. Є дуже простим в управлінні.
Винос конфіденційної інформації на носіях пам'яті, для особистого використання, втрата носія інформації з конфіденційними даними	**Right Management Services** – при виносі інформації за межі дії сервера Right Management Services, і спроби його відкрити документ буде неможливо прочитати. Документ зберігається в зашифрованому вигляді і відкривається в межах «видимості» Right Management Services сервера. **Термінальний режим роботи** – робота на віддаленому сервері, через тонкий клієнт. При правильному налаштуванні можна заборонити копіювати файли з термінального сервера, заборонити вихід в інтернет на термінальному сервері, заборонити використовувати буфер обміну між віддаленим сервером і локальним комп'ютером (тонким клієнтом) – це лише мала частина функцій , які використовуються для захисту інформації, але вже навіть цього достатньо, щоб присікти елементарні атаки.
Запис розмов співробітника, для запобігання витоку інформації через телефонну розмову	**Asterisk** або **Cisco Call Manager** налаштований на запис розмов і інтегрований з ERP або CRM системою. Також використовується в якості доказів, в спірних ситуаціях.

3. Захист конфіденційної інформації – одне з пріоритетних завдань сучасного бізнесу. Існують цілі методики з організації безпеки комерційно значимої інформації, установці потужного устаткування протидії зовнішнім атакам і хакерам, впровадження регламентів безпеки, інструкцій і рівнів допуску в корпоративному масштабі.

Потенційні загрози:

– крадіжка чи ушкодження електронних документів зсередини структури, самими співробітниками;

– втрата або крадіжка ноутбуків, «флешок», мобільних пристроїв співробітників з комерційно значущою інформацією, приміром, в громадських місцях, аеропортах, кафе і т.д.;

– проникнення у фінансові бази даних, злом електронних документів з комерційно значущою інформацією.

– використання вразливостей програмного забезпечення, особливо підкріплене повними правами адміністратора, які найчастіше надаються всім співробітникам.

Зазначені проблеми призводять до дуже серйозних наслідків і обов'язково повинні бути враховані при побудові інформаційної безпеки, підхід до їх вирішення має бути системний, з використанням інструментів групового контролю, шаблонів і політик безпеки, а саме:

а) шифрування файловий даних і систем:

– впровадження шифрованих файлових систем, таких як EFS;

– використання шифрованих апаратних сховищ – Qnap, HP, Synology, з крипто-модулями AES;

– впровадження софтверного ПО шифрування «на льоту» – CryptoPro, PGP, TrueCrypt.

б) шифрування ноутбуків, мобільних пристроїв і знімних носіїв

– використання програмних рішень – BitLocker, Kasperskiy, Endpoint Encryption, SecretDisk;

– використання дорожчих кінцевих пристроїв (ноутбуків, HDD і флеш-накопичувачів) з вбудованими модулями шифрування – рішення компаній Seagate, Asus, Sony.

в) захист своїх даних від системного адміністратора – за допомогою спеціалізованих рішень, таких як TrueCrypt можна створити структуру шифрованих «контейнерів» з захистом по паролю, програмному ключу або апаратному «брелоку», які дозволяють працювати з даними тільки призначеним особам.

г) обмеження доступу до електронних документів – надійним засобом обмеження доступу та захисту документів є Active Directory Rights Management Services, яке за допомогою маркування документів не допускає неправомірного їх використання. Службовці, які працюють з інформацією, тепер можуть вказувати тих, кому дозволено використовувати документ. Також вони можуть визначати дії, які дозволено виробляти з документом. Наприклад, вони можуть надати права на відкриття, внесення змін, друк, пересилання документа, а також на виконання ряду інших дій.

д) реєстрація мобільного пристрою на трекерах моніторингу – окремим пунктом можна відзначити рішення по реєстрації мобільного пристрою на спеціальних трекерах моніторингу географічного розташування, наприклад, Prey або за допомогою розширеної версії антивіруса Касперський. При втраті або крадіжці пристрою вказане прикладне ПО допоможе відстежити його поточне місце розташування, заблокувати доступ до модуля пам'яті або, в окремих випадках, знищити інформацію на ньому.

4. Забезпечення відмовостійкості і безперервності бізнес-процесів. Технологічне забезпечення безперервності бізнес-процесів – це, на думку компанії EFSOL, практично першочергове завдання IT системи [5].

Можливість будь-якої системи зберігати свою працездатність після відмови або виходу з ладу одного або декількох складових компонентів називається відмовостійкістю системи.

Таблиця 3

Основні проблеми відмовостійкості бізнес-процесів [6; 7; 8; 9]

Проблема	Рішення
Відмовостійкість інтернет каналів	Рекомендується мати мінімум 2 стабільних каналу інтернет від двох незалежних провайдерів, притому, один з них - з фізичної лінії, а другий - по бездротової радіолінії. Таким чином, виключаються ризики: Фізичного пошкодження одночасно двох кабелів різних провайдерів; Вплив форс-мажорів локального характеру, наприклад збій комутаційного вузла; Проблеми з маршрутизацією і стабільністю каналу у одного провайдера.
Відмовостійкість шлюзів інтернет і віддаленого доступу	Дані ключові вузли рекомендується створювати на апаратних професійних рішеннях з можливістю об'єднання обох пристроїв у відмовостійкий кластер. Така архітектура зможе забезпечити стабільність зв'язку компанії з простором Інтернет, з'єднання з філіями і безперервний доступ до внутрішніх і зовнішніх ключовим сервісів.
Відмовостійкість проксі-серверів	В різних системах реалізована за допомогою або синхронізації конфігураційних файлів, або шляхом об'єднання кількох служб в пул.
Відмовостійкість системи зберігання даних	Всі професійні системи зберігання даних основних світових брендів-виробників містити повністю дубльовану апаратну структуру. Це значить, що система продовжить функціонувати при виході з ладу будь-якого її компоненту.
Відмовостійкість апаратних носіїв	Забезпечується за рахунок єдиного кластера віртуальних машин з технологією «живої міграції». Дана функція присутня в основних відомих гіпервізорами: Vmware, Hyper-V, Xen
Відмовостійкість термінальних серверів	При виході з ладу одного термінального сервера, сесії користувачів автоматично перемикаються на другий термінальний сервер, і користувачі продовжують працювати. Це забезпечується службою розподільника термінальних сесій (TS Broker), яка встановлена на контролерах домену.
Відмовостійкість системи управління базами даних (СУБД) серверів	Реалізується за допомогою єдиного сховища даних. Приміром, технологія кластеризації Microsoft SQL Server об'єднує дві віртуальні машини серверів СУБД в один кластер з єдиними віртуальною IP-адресою і базою даних. При виході з ладу основного SQL сервера запити автоматично переводяться на резервний. Аналогічним чином побудована «архітектура високої готовності» IBM DB2 і Oracle Real Application Clusters (RAC). У більш бюджетних СУБД, таких як PostgreSQL і MySQL також існує поняття кластеризації. Вона досягається за рахунок потокової реплікації баз в режимі Master-Slave і єдиними віртуальним IP-адресою.
Відмовостійкість серверів додатків ERP	Сервера додатків у різних ERP системах мають приблизно схожі технології відмовостійкості - можливість одночасного підключення і рівномірного розподілу клієнтських з'єднань між усіма серверами додатків. Це просте рішення дає в своїй реалізації як відмовостійкість так і приріст обчислювальної потужності всього пулу додатків ERP.
Відмовостійкість контролерів домену	Реалізована за допомогою штатного механізму основного і резервного ролей контролерів домену.
Відмовостійкість файлових серверів	На MS Windows може бути реалізована за допомогою повноцінної кластерізірованної ролі Microsoft, що дозволяє забезпечити доступ до файлових даними практично безперервно. На інших операційних системах існують свої власні технології забезпечення цілодобової доступності до даних, починаючи від розподіленої файлової системи, закінчуючи онлайн репликацією master-slave.
Відмовостійкість пошти та сервера документообігу	Принцип дублювання сервісів пошти і документообігу в крупних професійних системах (MS Exchange, Lotus) побудований на класичному розподілі ролей на рівні – транспортний, зберігання, одержання і т.д. На даних рівнях створюються так звані групи високої доступності, які і забезпечують підстраховку кожного з вузлів системи. У більш лінійних системах кластеризація відбувається шляхом резервування основних конфігураційних параметрів і файлових баз даних за принципом master-slave. Ця система більше походить на «холодний резерв» і користується популярністю в малому бізнесі.
Відмовостійкість web-сервісів	Може бути реалізована шляхом резервування за рівнями: Рівень з'єднань – застосування механізмів відстеження сесій при кластеризації служби web (механізм NLB - Network Load Balancing); Рівень параметрів web – онлайн реплікація конфігураційних файлів web-сервісів; Рівень даних – застосування єдиного сховища для баз даних забезпечить доступ при виході з ладу одного з web-серверів.
Відмовостійкість корпоративного порталу	У великих професійних системах корпоративних порталів відмовостійкість сервісу реалізується за рахунок архітектури високої доступності кожного з компонентів порталу та застосування концепції «єдина ферма»

Відмовостійка система повинна зберігати свою працездатність при виході з ладу мінімум одного вузла, відповідно, основний спосіб підвищення відмовостійкості – створення апаратної надмірності шляхом резервування.

Сучасним комплексним вирішенням проблеми високодоступних сервісів для бізнесу є професійна система зберігання даних (СЗД). До неї підключаються парами оптичні комутатори і апаратні обчислювальні модулі (простіше кажучи, сервера без власних

жорстких дисків). Виробляється перехресна комутація всіх вузлів даної системи. Таке моделювання ІТ-структури може дати гарантію збереження корпоративних даних при виході з ладу будь-якого апаратного компонента. Основні елементи цієї системи представлені у табл. 3.

Переваги системи відмовостійкості для бізнесу:

а) безперервність робочих процесів. Дані технології забезпечують резервування критичних сервісів в режимі онлайн. Це означає, що при виникненні будь-яких проблем з основними ресурсами вся система миттєво переключається на резервні практично непомітно для користувача. Це дозволяє уникнути простоїв компанії та фінансових втрат.

б) економічна ефективність. Кластера по суті є самодостатніми системами. При виникненні аварійних ситуацій кластер розрахований на автоматичні дії щодо їх усунення та підтримці працездатності сервісів. Відповідно, немає необхідності оплачувати цілодобову роботу фахівців і чергових техніків для відпрацювання можливих аварій вручну, що дозволить істотно економити великі бюджети фонду оплати праці.

в) захист цілісності даних. Структура відмовостійких ІТ-систем побудована таким чином, що всі важливі дані компанії знаходяться в «серце» кластера – надійній системі зберігання даних. Решта сервера потрібна тільки для оперативної обробки інформації та інтерактивної роботи з системою. Це значить, що при виході з ладу одного з серверів він може бути з легкістю замінений без ризику втрати чи пошкодження інформації компанії.

г) альтернативне використання резервних потужностей. Одночасно з відмовостійкостю забезпечується також розподіл оперативної навантаження по всім учасникам кластеру. Дана схема дозволяє використовувати всі потенційні потужності, які не закуповуючи додаткове цільове обладнання і не роздуваючи ІТ-структуру. З урахуванням вартості сучасних серверних рішень подібна оптимізація структури може приносити компанії десятки тисяч доларів економії.

Рано чи пізно перед будь-якою організацією, незалежно від форми власності та виду діяльності, стає питання захисту інформації від витоку. У кожної компанії є свої дані, які є основою її діяльності, її комерційною таємницею. Крадіжка або розголошення цієї таємниці призведе до негативних наслідків для компанії. Частково вирішити цю проблему допоможе використання саме сучасних засобів, як програмних, так і технологічних.

Література:

1. Bashynskaya I. Organization of the ensuring the informational and analytical safety at the enterprise / Institutionelle Grundlagen für die Funktionierung der Ökonomik unter den Bedingungen der Transformation: Sammelwerk der wissenschaftlichen Artikel.Vol. 2 – Verlag SWG imex GmbH, Nürnberg, Deutschland, 2014. – S. 216-218
2. Башинська І.О. Розділ 4.2. Сучасні засоби забезпечення інформаційної складової економічної безпеки промислового підприємства (С. 310-315) у кол. монографії Формування механізму стійкого розвитку економіки: теорія та практика : - Дніпропетровськ: "ФОП Дробязко С.І.", 2014. - 438 с.
3. Башинська І.О. Розділ 3.2. Уточнення визначення дефініції та економічного змісту категорії «економічна безпека підприємства» (С. 14-20) у кол. монографії Економічна безпека в умовах глобалізації світової економіки: [колективна монографія у 2т.]. – Дніпропетровськ: «ФОП Дробязко С.І.», 2014. – Т. 2. – 349 с.
4. Баланда А.Л. Інформаційно-аналітичне забезпечення економічної безпеки суб'єктів підприємницької діяльності: стан та перспективи розвитку / А.Л. Баланда // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2011. – № 1(37). – С. 150-155. - Режим доступу: http://www.pmdp.org.ua/images/Journal/37/11balspr.pdf
5. Сайт компанії EFSOL [електроний ресурс]. Режим доступу: http://efsol.livejournal.com/
6. Speranskyy V.O. Identification of Nonlinear Dynamical Systems Using Volterra Model with Interpolation Method in Frequency Domain/ Pavlenko V.D. // Electrotechic and Computer Systems. – 2012. – № 05 (81). – P. 229-234.
7. Шелковников Б. М., Ботулінський С. М. Підвищення ефективності роботи Microsoft Hyper-V Live Migration на відстані / Б. М. Шелковников, С. М. Ботулінський // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – № 2 (18). – С. 43-48
8. Бабенко Г. В. Анализ современных угроз безопасности информации, возникающих при сетевом взаимодействии // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2010. – № 2. – С. 149-152

9. Сурженко Д.О. Математичне моделювання динамічних процесів у комп‘ютерних мережах / Д.О. Сурженко, М.В. Кліпаков // Вісник Східноукраїнського національного університету імені В. Даля. – Луганськ: Вид-во СНУ, 2013. – №6(195). – Частина 1. – С. 184-188.
10. Петрик В. М., Кузьменко А. М., Остроухов В. В. та ін. Соціально-правові основи інформаційної безпеки: Навчальний посібник / За ред. В. В. Остроухова. – К.: Росава, 2007. – 496 с.

ГЛАВА 2.2. РОЗВИТОК КРЕДИТНИХ СПІЛОК В КОНТЕКСТІ СКЛАДАННЯ ІНТЕГРОВАНОЇ ЗВІТНОСТІ

Гриценко О.І.
к.е.н., доцент кафедри бухгалтерського обліку і аудиту
ДВНЗ «Українська академія банківської справи Національного банку України»

Кредитні спілки є важливою інфраструктурною складовою фінансового ринку. Тому їх господарська діяльність повинна сприяти економічному розвитку регіону. При організації кредитних відносин кредитні спілки виходять з необхідності врахування інтересів спілки, її пайовиків, позичальників та загальнодержавних інтересів.

Однією з найбільш суттєвих проблем в сучасній кредитній справі, в тому числі у діяльності кредитної спілки, є залучення та підтримка достатнього обсягу капіталу, обчислення його послідовного збільшення. Крім того, в Україні кредитна спілка визнана не кооперативом, як в інших державах, а громадською організацією, що створює певні перешкоди для відродження цієї форми кредитної кооперації.

В умовах формування конкурентного середовища і розвитку конкуренції в галузі перед кредитними кооперативами постає завдання розробити конкурентну стратегію.

Метою розробки конкурентної стратегії не є досягнення запланованих конкретних цифр, розрахунок і аналіз яких роблять у процесі діяльності підприємства. Найважливішим у формуванні стратегії є ретельний аналіз стану конкурентного середовища та діяльності кредитних кооперативів.

Розробка конкурентної стратегії складається, як правило, з таких етапів:

– аналіз стану конкурентного середовища в галузі;

– аналіз стану підприємства порівняно з конкурентами;

– стратегічне планування;

– реалізація конкурентної стратегії та її оцінка.

Конкурентна стратегія полягає в тому, щоб максимально гнучко задовольняти невеликі за обсягом (локальні) потреби ринку. Оцінити ефективність розробленої конкурентної стратегії можна зазвичай за допомогою аналізу «вартість – ефективність», мета якого полягає в прагненні порівняти обсяги доходів на одиницю ресурсу, його буде використано для кожного із запланованих заходів. Дану методику не можна застосувати до кредитних спілок, оскільки мета їх діяльності полягає у збереженні вкладів і задоволенні потреб її членів у позикових коштах.

Потреба пошуку нетрадиційних методів вирішення проблеми підвищення конкурентоспроможності кредитних спілок є дуже актуальною і значимою. Одним із таких методів є запровадження рейтингової оцінки як серед членів спілки, так і через порівняння аналогічних суб'єктів господарювання на ринку кредитних послуг.

Цікавими й корисними у вирішенні проблеми формування кооперативного сектора є дослідження В. Зіновчука, В. Гончаренко, Ф.Горбонос, Л. Молдаван, А. Пантелеймоненко, Ю. Ушкаренко, М. Маліка, П. Саблука, С. Юрій. Завдяки працям цих учених сформульовано підґрунтя для подальших наукових досліджень. Можна зазначити, що кооперація досить широко відображена в наукових публікаціях, але залишається чимало дискусійних проблем, що потребують розширення і поглиблення наукового пошуку.

Метою даного дослідження є визначення перспектив покращання конкурентоспроможності кредитної кооперації в Україні через впровадження інтегрованої звітності.