МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
Доктор економічних наук, доцент
_____ С.В. Легомінова
«___»_____20__ р.

До захисту
Завідувач кафедри УІКБ
Доктор економічних наук, доцент
_____ С.В. Легомінова
«___»_____20__ р.

ДИПЛОМНА РОБОТА
на тему:

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ОСОБЛИВОСТІ ЇЇ ОРГАНІЗАЦІЇ

СТУДЕНТ: Гришко Ростислав Олександрович _____
(підпис)

КЕРІВНИК: к. т. н., доцент Дзюба Тарас Михайлович _____
(підпис)

НОРМОКОНТРОЛЕР: _____ _____
(підпис)

Київ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Освітньо-кваліфікаційних рівень – магістр
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
(підпис)
“___”_____ 2020 р.

ЗАВДАННЯ
на дипломну роботу
студенту Гришку Ростиславу Олександровичу

1. Тема роботи «ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ОСОБЛИВОСТІ ЇЇ ОРГАНІЗАЦІЇ», затверджена наказом по університету від « 13 » жовтня 2020 р. № 230.

2. Термін здачі студентом оформленої роботи « 10 » січня 2021 р.

3. Об’єкт дослідження: інформаційна безпека підприємства.

4. Предмет дослідження: особливості організації інформаційної безпеки підприємства.

5. Мета дослідження: дослідження особливостей організації інформаційної безпеки підприємства.

6. Перелік питань, які мають бути розроблені:

6.1. Провести аналіз основних принципів організації інформаційної безпеки на підприємстві.

6.2. Використовуючи методи тестування та аналізу інформаційної системи підприємства, обґрунтувати рекомендації щодо доцільних способів організації інформаційної безпеки на підприємстві.

6.3. Розробити рекомендації щодо доцільних способів організації та управління інформаційною безпекою підприємства.

7. Дата видачі завдання «14» жовтня 2020 р.

РЕФЕРАТ

Дипломна робота присвячена дослідженню особливостей організації інформаційної безпеки підприємства. Робота складається зі вступу, трьох розділів, що містять 11 рисунків, 2 таблиці та 11 формул, висновків та списку використаних джерел, що містить 41 найменувань. Загальний обсяг роботи становить 82 аркуші, з яких 8 займають ілюстрації та блок-схеми, а також перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження в роботі є процес організації управління інформаційною безпекою підприємства.

Метою роботи є розгляд особливостей організації інформаційної безпеки підприємства.. Для цього у роботі використовуються методи теорії інформаційної безпеки, теорії управління інформаційною безпекою, методи розробки та тестування надійного програмного середовища.

Як результат в роботі були розглянуті основні принципи організації інформаційної безпеки підприємства, було розглянуто методи тестування та аналізу стану інформаційної безпеки також опрацьовано комплекс принципів та засобів, що дозволять спроектувати, використовувати та підтримувати інформаційну систему підприємства на належному рівні.

Сфера застосування. Матеріали та результати роботи можуть бути використані при плануванні та реалізації інформаційної безпеки для будь-якого підприємства.

Ключові слова: БЕЗПЕКА, БЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗИ, ТЕСТУВАННЯ, ІНФОРМАЦІЯ, ЗАХИСТ, ІНФОРМАЦІЙНА СИСТЕМА, УПРАВЛІННЯ РИЗИКАМИ.

ЗМІСТ Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

CDR	-сервер детальної реєстрації викликів
DDoS	- Distributed Denial of Service
DoS	- Denial of Service
FMS	-сервер Frod-management
АС	-автоматизована система
ІБ	-інформаційна безпека
ІС	-інформаційна система
ІТС	-інформаційно-телекомунікаційна система

ВСТУП

А к т у а л ь н і с т ь д о с л і д ж е н н я. На сьогоднішній день нагальною постає проблема збільшення інформаційної безпеки підприємства, яка значною мірою залежить від ступеня захищеності інформаційної сфери. Рівень організації інформаційної безпеки впливає на розвиток та впровадження науково-технічних інновацій у процеси виробництва, збереження стабільності функціонування можливості економічного зростання.

Під впливом глобальних процесів спостерігається прискорення науково-технічного прогресу, кількість оброблюваної інформації, розширюється обмін новими процесами. Проте під швидкими темпами зростання економічних та технічних процесів при здійсненні господарської діяльності зростає і роль інформаційної безпеки підприємства.

При веденні своєї діяльності підприємець обов’язково наштовхується на необхідність отримання, обробки, зберігання, перетворення, передачі та ліквідації непотрібної інформації. Якщо деяка інформація є цінною для підприємця, то її треба охороняти від зловмисників. При захисті інформації слід перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на усіх носіях, що маються на підприємстві.

М е т а і з а в д а н н я д о с л і д ж е н н я. **Мета роботи** полягає в розгляді особливостей та організації інформаційної безпеки підприємства. Для досягнення цієї мети потрібно виконати такі **завдання**:

1) Розглянути основні принципи організації інформаційної безпеки на підприємстві;

2) Проаналізувати методи тестування та аналізу інформаційної системи підприємства;

3) Розробити загальні принципи організації та управління інформаційною безпекою підприємства.

Виходячи з такого, у роботі **об'єктом дослідження** є процес організації управління інформаційною безпекою підприємства. **Предмет дослідження** є методи, засоби та принципи захисту інформації на підприємстві та рекомендації щодо концепції безпеки підприємства.

Методи дослідження. Для вирішення описаного вище наукового завдання в роботі використані методи теорії інформаційної безпеки, теорії управління інформаційною безпекою, методи розробки та тестування надійного програмного середовища.

Наукова новизна одержаних результатів. Новими науково-обґрунтованими результатами, які отримані в роботі, є:

1) Рекомендації щодо використання моделей тестування на надійність програмного забезпечення в інформаційних системах;
2) Загальні принципи побудови системи безпеки підприємства;
3) Використання програмного середовища для одержання аналізу аномалій мережевого трафіку інформаційно-обчислювальних систем.

Практичне значення одержаних результатів. Нові наукові результати, отримані в роботі, у сукупності складають підґрунтя для організації надійної інформаційної безпеки для нових підприємств та модернізації та покращення стану інформаційної безпеки для уже функціонуючих підприємств.

Розділ 1

ОСНОВНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

1.1 Сутність та поняття інформаційної безпеки підприємства

Успішність функціонування підприємств у динамічному ринковому середовищі значною мірою визначається станом інформаційної безпеки. Рівень економічної безпеки суб'єкта господарювання залежить від того, наскільки ефективною є інформаційна безпека суб'єкта господарювання, що дасть змогу уникнути можливих загроз та негативних наслідків впливу конкурентного середовища. Більшість науковців вважають, що безпека підприємства – це такий стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантується найбільш ефективне їхнє використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім та зовнішнім негативним впливам (загрозам). Відповідно достатній рівень інформаційної безпеки дасть змогу підприємству повною мірою використовувати необхідну інформацію для прийняття результативних управлінських рішень, виконання яких обумовить подальшу фінансову стійкість підприємства і буде сприяти його подальшій ефективній роботі[16].

Згідно законодавства України інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.[31].

Слід зазначити, що задоволення в будь-якому ступені потреб в інформації призводить до оволодіння відомостями про навколишній світ і процеси, що протікають в ньому, тобто інформованості особистості, суспільства і держави.

Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і, як наслідок, обґрунтованість рішень і дій, які приймаються.

Залежно від виду загроз (рис. 1.1.) інформаційну безпеку можна розглядати наступним чином:

- як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод громадянина.

Рис. 1.1. Загрози інформаційній безпеці

Питання інформаційної безпеки, які наведені в юридичній та спеціальній літературі, і базуються на розумінні інформаційної безпеки як складової національної безпеки України. По суті це є вірним, оскільки завданням заходів з інформаційної безпеки є мінімізація шкоди за неповноти, несвоєчасності або недостовірності інформації чи негативного інформаційного впливу через наслідки

функціонування інформаційних технологій, а також несанкціоноване поширення інформації. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, встановлених міжнародним і вітчизняним законодавством.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення і нейтралізацію тих обставин, факторів і дій, які можуть задати збиток або перешкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.[31].

1.2 Методи забезпечення безпеки інформації на підприємстві

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, за допомогою якого засоби інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів підприємств та організацій.

Тому необхідно чітке юридичне оформлення при розробці нормативних актів, що регулюють діяльність органів інформаційної безпеки. Найважливіша вимога до обґрунтування способів, форм та механізмів їх реалізації полягає в абсолютному верховенстві права в будь-якій діяльності.[14]

Забезпечення інформаційної безпеки має бути спрямоване перш за все на запобігання ризиків, а не на ліквідацію їх наслідків. Саме прийняття запобіжних заходів для забезпечення конфіденційності, цілісності, а також доступності інформації і є найбільш правильним підходом у створенні системи інформаційної безпеки. Будь-який витік інформації може призвести до серйозних проблем для компанії – від значних фінансових збитків до повної ліквідації.

Одним з базових, основних елементів системи інформаційної безпеки промислових підприємств виступають принципи, які мають бути покладені в основу її побудови. Для промислових підприємств основними принципами ІБ є наступні див. рис. 1.2. :

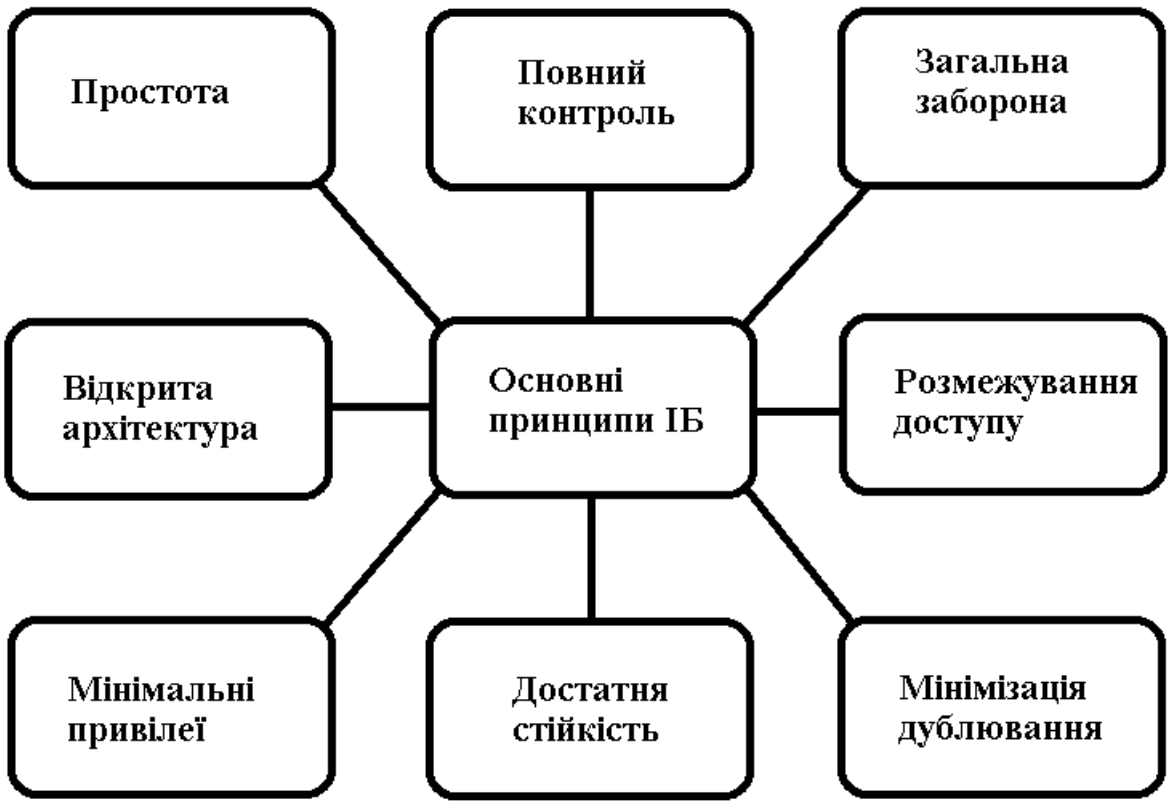

Рис. 1.2. Основні принципи інформаційної безпеки

Розглянемо принципи ІБ докладно:

- Простота. Цей принцип ІБ наголошує на тому, що простота використання інформаційної системи здатна забезпечити мінімізацію помилок. Процес експлуатації інформаційної системи обов’язково супроводжується ненавмисними помилками з боку користувачів та адміністраторів системи, результатом яких може стати зниження рівня ІБ. Зрозуміло, що ускладнення здійснюваних користувачами та адміністраторами операцій і процедур призводить до зростання кількості таких помилок. Для зниження кількості

помилок простота використання системи є необхідною умовою. Проте, простота використання не означає простоту архітектури і зниження вимог до функціональності системи ІБ.

- Повний контроль. Виконання цього принципу передбачає організацію безперервного контролю за станом ІБ та моніторинг всіх подій, що впливають на ІБ. Повний контроль передбачає таку архітектуру системи ІБ, яка б дозволяла здійснювати контроль доступу до будь якого об’єкту ІС, блокувати небажані дії та швидко відновлювати нормальні параметри інформаційної системи.
- Загальна заборона. Заборонено все, на що немає дозволу. Доступ до об’єктів ІС можливий тільки при наявності відповідного дозволу, який надається у відповідності до діючих нормативних документів щодо організації роботи ІС. Проте важливо усвідомлювати, що система ІБ спрямована на надання дозволу, а не заборони будь яких дій. Означений принцип передбачає, що в ІС можливо виконання тільки відомих безпечних дій. Система не налаштовується на пошук та розпізнавання будь-якої загрози, оскільки такий шлях побудови системи ІБ є дуже ресурсномістким, та унеможливлює забезпечення достатнього рівня ІБ.
- Відкрита архітектура ІС. Цей принцип інформаційної безпеки полягає у тому, що безпека повинна забезпечуватися через неясність. Спроби захистити інформаційну систему від комп'ютерних загроз шляхом ускладнення, заплутування і приховування слабких місць ІС, опиняються в кінцевому підсумку неспроможними і тільки відстрочують успішну хакерську, вірусну чи інсайдерську атаку.
- Розмежування доступу. Даний принцип ІБ полягає в тому, що кожному користувачеві надається доступ до інформації і її носіїв у відповідності з його повноваженнями. При цьому виключена можливість перевищення повноважень. Кожній ролі/посади/групі можна призначити свої права на виконання дій (читання/редагування/видалення) над певними об'єктами ІС.
- Мінімальні привілеї. Принцип мінімальних привілеїв полягає у виділенні користувачеві найменших прав і доступу до мінімуму необхідних

функціональних можливостей програм. Такі обмеження, тим не менш, не повинні заважати виконанню роботи.

- Достатня стійкість. Цей принцип інформаційної безпеки виражається в тому, що потенційні зловмисники повинні зустрічати перешкоди у вигляді досить складних обчислювальних завдань. Наприклад, необхідно, щоб злом паролів доступу вимагав від хакерів неадекватно великих проміжків часу і/або обчислювальних потужностей.
- Мінімізація дублювання. Передбачає мінімізацію ідентичних процедур. Цей принцип інформаційної безпеки полягає в тому, що в системі ІБ не повинно бути загальних для декількох користувачів процедур, таких як введення пароля. У цьому випадку масштаб можливої хакерської атаки буде менше [9].

Побудована за наведеними принципами система ІБ має бути налаштована на досягнення визначених цілей, специфіка яких буде великою мірою визначати як структуру системи так і основні параметри її функціонування. Для підприємства основними цілями досягнення високого рівня інформаційної безпеки є забезпечення конфіденційності, цілісності, доступності, достовірності та неспростовності інформації.

1.3 Основні складові інформаційної безпеки

Інформаційна безпека – багатогранна, можна навіть сказати, багатовимірна область діяльності, в якій успіх може принести тільки систематичний, комплексний підхід. Спектр інтересів суб’єктів, зв’язаних з використанням інформаційних систем, можна розділити на наступні категорії: забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів і підтримуючої інфраструктури.

Основними складовими інформаційної безпеки є поняття доступності, цілісності і конфіденційності.

Доступність - це можливість за прийнятний час одержати необхідну інформаційну послугу. Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни. Нарешті, конфіденційність - це захист від несанкціонованого доступу до інформації.

Інформаційні системи створюються (отримуються) для отримання певних інформаційних послуг. Якщо з тих або інших причин надати ці послуги користувачам стає неможливим, то це очевидно, завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ця складова виділяється як найважливіший елемент інформаційної безпеки.

Особливо яскраво роль доступності виявляється в різного роду системах управління - виробництвом, транспортом і т.п. Зовні менш драматичні, але також вельми неприємні наслідки - і матеріальні, і моральні - може бути тривала неприступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних і авіаквитків, банківські послуги і т.п.).

Цілісність можна підрозділити на статичну (що розуміється як незмінність інформаційних об'єктів) і динамічну (що відноситься до коректного виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність виявляється найважливішим аспектом ІБ в тих випадках, коли інформація служить "керівництвом до дії". Рецептура ліків, медичні процедури, набір і характеристики комплектуючих виробів, що наказали, хід технологічного процесу - все це приклади інформації, порушення цілісності якої може виявитися в буквальному розумінні смертельним.

Конфіденційність – найбільш опрацьований у нашій країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем пов’язана із серйозними труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, тому більшість користувачів позбавлено можливості мати уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони і технічні проблеми.

Якщо повернутися до аналізу інтересів різних категорій суб’єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй по важливості цілісність.[24].

1.4 Структурний аналіз інформаційного середовища та загальна характеристика ризиків інформаційної безпеки підприємства

Інформаційне середовище підприємства формують інформаційні системи та користувачі. Інформаційні системи складаються із трьох основних елементів:

- устаткування;
- програмне забезпечення;
- дані.

До устаткування, зокрема, належать:

- сервери;
- мережеві пристрої;
- пристрої для зберігання даних;
- комп’ютерні термінали;

- інше спеціалізоване обладнання.

В цілому, до устаткування відноситься комп’ютерне та інше обладнання, телекомунікаційні кабелі, приміщення тощо. Устаткування є речовим вираженням інформаційної системи.

Програмне забезпечення складається із таких частин:

- операційна система;
- система управління, аналізу та обробки баз даних;
- антивірусне програмне забезпечення.

Під операційною системою прийнято розуміти базовий комплекс програм, що виконує управління апаратною складовою комп'ютера або віртуальної машини, забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем [35]. У операційній системі відбуваються такі види процесів:

- експлуатаційні;
- робочі;
- обслуговуючі;
- пов’язані із розвитком.

Дані процеси становлять найбільшу частку процесів операційної системи. До них відносяться найпоширеніші, повторювані процеси, які, не вимагають особливої користувацької компетентності. Робочі процеси забезпечують постійну підтримку користувачів, діагностику і моніторинг інформаційної системи в цілому. Обслуговуючі процеси покликані забезпечити доступність, продуктивність і безперервність функціонування інформаційної системи у середньостроковій і довготривалій перспективі.

Процеси, пов’язані із розвитком – це ті, у межах яких відбувається планування змін у інформаційній системі, генерування та запровадження нових рішень.

Додатки є програмним забезпеченням, яке використовується з метою обробки даних відповідно до потреб, представлення даних у необхідній формі тощо. Додатки, які використовуються у інформаційно-технологічному супроводі підприємницької діяльності, можна класифікувати за їхніми функціями, тобто напрямками (сферами, завданнями) впливу на функціонування бізнесу. Зокрема, додатки можуть стосуватися:

- планування ресурсів підприємства;
- бухгалтерського обліку і фінансової звітності;
- взаємодії з клієнтами;
- логістики;
- виробництва;
- управління персоналом тощо.

Як бачимо, додатки інтегровані практично з усіма бізнес-процесами. Застосування додатків сприяє гармонізації процесів, які відбуваються на підприємстві, підвищенню їхньої ефективності. Під даними у інформатиці розуміють інформацію, подану у формалізованому вигляді, придатному для обробки (інтерпретації) автоматичними засобами за можливої участі людини [1-2].

Наступним елементом інформаційного середовища підприємства є користувачі. Користувачі класифікуються за рівнем (сферою) доступу до складових інформаційної системи. Так, левова частка користувачів у межах підприємства переважно безпосередньо використовує додатки та опосередковано взаємодіє із системою управління базами даних (наприклад, при створенні чи поширенні інформації). Тільки окремі користувачі наділяються доступом до операційної системи [12].

За характером взаємодії (взаємовідношення) із конкретним підприємством серед користувачів інформаційної системи підприємства можна виділити:

- власників;

- працівників;
- осіб, які надають послуги підприємству (на цивільно-правовій основі, періодично або за необхідності);
- клієнтів підприємства (покупців, замовників тощо);
- партнерів підприємства (контрагентів, з якими підприємство співпрацює на договірній основі).

Запропонований перелік не претендує на вичерпність та включає лише найбільш розповсюджені, універсальні групи користувачів інформаційної системи підприємства за звичайних обставин [10].

Окрім вже наведеної класифікації, доцільно також розрізняти користувачів інформаційної системи підприємства за фактором легальності їхнього доступу до ІС (як в цілому, так і щодо окремих елементів). Відповідно, користувачі можуть бути:

- санкціонованими;
- несанкціонованими [21].

Саме у контексті взаємозв’язку окремих елементів інформаційної системи підприємства між собою, а також взаємодії користувачів з інформаційною системою підприємства (чи окремими її складовими) доцільно говорити про кібербезпеку, або ж безпеку інформаційної системи у межах конкретного бізнесу.

Під останньою прийнято розуміти стан захищеності устаткування, програмного забезпечення і, власне, даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, можливість її використання для визначених цілей.

У свою чергу, забезпечення кібербезпеки передбачає:

- запобігання внутрішньо-системних ризиків інформаційної системи;
- запобігання негативного впливу зовнішнього середовища на функціонування інформаційної системи;

- запобігання шкідливого впливу людей і зокрема, користувачів [7].

Під внутрішньо-системними ризиками маються на увазі порушення функціонування інформаційної системи, обумовлені недосконалостями самої інформаційної системи, без будь-якого зовнішнього впливу. Серед цієї категорії ризиків окремо можна виділити збої, тобто порушення нормального функціонування інформаційної системи в цілому чи окремих її складових, і окремо – загрози для цілісності, конфіденційності, доступності та/або можливості цільового використання інформації, які існують при нормальній роботі інформаційної системи або її елементів [18].

Суттєво, що відсутність зовнішнього впливу у контексті внутрішньо-системних ризиків інформаційної системи є доволі умовною характеристикою. Так, будь-яка інформаційна система (чи окремий її елемент) має свого розробника, а відтак, саме його помилкою або недалекоглядністю часто обумовлені системні збої, а тим більше, не пов’язані зі збоями внутрішньо-системні загрози. Під негативним впливом зовнішнього середовища як фактором ризику для кібербезпеки підприємства маються на увазі чинники, які безпосередньо не пов’язані ані з функціонуванням інформаційної системи самим по собі, ані з взаємодією користувачів з інформаційної системи.

Зокрема, ідеться про цілісність і справність устаткування, безпеку приміщень, у яких воно знаходиться, тощо. Перелік чинників ризику у цьому контексті необмежений: відповідні чинники можуть мати метеорологічний, геологічний, астрономічний, механічний, зоологічний, електричний та інший характер [8].

Шкідливий вплив людей на функціонування інформаційної системи підприємства може бути вчинений як умисними, так і необережними діями чи бездіяльністю. При цьому умисел може стосуватися як безпосередньо реалізації ризиків кібербезпеки, так і заподіяння підприємству шкоди іншого характеру. Наприклад, крадіжка устаткування (у розумінні – елемента інформаційної

системи) підприємства для його продажу (з корисливою метою) хоч і не здійснюється з наміром порушення цілісності, конфіденційності, доступності та/або можливості цільового використання інформації, проте призводить до відповідних наслідків. При цьому люди, які здійснюють шкідливий вплив на функціонування інформаційної системи, не є користувачами [15].

Також суттєво, що користувачами інформаційної системи можуть бути не лише люди, але і боти (програми), юридичні особи тощо. Проте усі неантропологічні користувачі інформаційної системи, врешті, все одно зводяться до людини чи групи людей [18].

Превенція внутрішньо-системних ризиків, негативного впливу зовнішнього середовища та шкідливих діянь людей і/зокрема користувачів є взаємопов’язаними заходами, здійснення яких необхідне для забезпечення інформаційної безпеки підприємства. Ефективність цих заходів можлива лише за умови їхнього комплексного застосування. Реалізація ризиків кібербезпеки підприємства може мати наступні наслідки:

- витік інформації;
- втрата цілісності інформації;
- модифікація (зміна) інформації;
- втрата доступу інформації для санкціонованих користувачів тощо.

Усі ці наслідки є шкідливими для функціонування бізнесу в цілому. Так, наприклад, витік інформації передбачає порушення її режиму. Зокрема, ідеться про таємну, конфіденційну та службову інформацію, яка охороняється законом, іншими актами, у тому числі локальними (прийнятими та чинними в межах конкретного підприємства чи організації).

Оприлюднення відповідної інформації може завдати шкоди законним інтересам, діловій репутації підприємства, а в окремих випадках навіть стати приводом для застосування до нього заходів юридичної відповідальності. Останнє можливо, наприклад, за умови протиправного розповсюдження персональних

даних, володільцем чи розпорядником яких є підприємство, або ж таємної (комерційна таємниця) чи конфіденційної інформації контрагентів підприємства, яка стала відома у процесі договірної співпраці [36].

Втрата цілісності інформації спотворює базу для прийняття важливих для бізнесу рішень, а модифікація інформації може обумовити прийняття рішень, які в подальшому завдадуть шкоди підприємству. Недоступність інформації для санкціонованих користувачів унеможливлює злагоджене функціонування підприємства та послідовно гальмує, а то і перериває низку бізнес-процесів [19].

По суті, спектр загроз кібербезпеки підприємства розширюється пропорційно розвитку інформаційних технологій в цілому. Відповідно, з кожним днем з'являються нові ризики, часто дедалі витонченіші, тобто складніші для виявлення і протидії та масштабніші за наслідками реалізації. Останнім часом у інформатиці та юриспруденції закріпилося поняття кіберзлочинності. Так, під кіберзлочинами розуміють правопорушення, у ході яких здійснюється викрадення, спотворення, знищення інформації, розміщеної у інформаційній системі. При цьому заподіяння шкоди інформаційній системі може бути як кінцевою метою вчинення злочину (суб'єктивною стороною злочину), так і способом досягнення іншої злочинної мети (об'єктивною стороною злочину).

Найчастіше кіберзлочини вчиняються із корисливих, а також із хуліганських мотивів. Ці злочини називають також інформаційними [38].

Для прикладу, Інтерпол використовує таку класифікацію кіберзлочинів:

- несанкціонований доступ та перехоплення;
- ухилення від плати за користування (так звана крадіжка часу);
- комп'ютерний вірус;
- зміна комп'ютерних даних;
- шахрайство з банкоматами;
- комп'ютерне шахрайство;
- незаконне копіювання;

- телефонне шахрайство;
- комп’ютерний саботаж;
- комп’ютерна підробка та інші [23].

Конвенція Ради Європи по боротьбі з кіберзлочинністю, яка, до речі, ратифікована вищим законодавчим органом України, групує інформаційні злочини наступним чином:

- злочини проти конфіденційності, цілісності та доступності інформаційних систем (зокрема, даних);
- шахрайство та підробка, пов’язані із використанням комп’ютерів;
- злочини, пов’язані із протиправним розміщенням інформації у мережах (зокрема, протиправної інформації);
- злочини проти авторських та суміжних прав [35].

Кримінальний кодекс України визначає всього чотири різновиди складу злочину, безпосередньо пов’язаних із сферою безпеки інформаційних систем, зокрема:

- несанкціоноване втручання у роботу комп’ютерів, мереж, автоматизованих систем (ст. 361);
- створення та розповсюдження вірусів (ст. 361-1);
- зловживання правом доступу до інформації, яка обробляється у комп’ютерах, мережах, автоматизованих системах, під яким розуміється протиправне надання доступу до відповідної інформації стороннім особам (ст. 361-2);
- несанкціоновані дії з інформацією, яка обробляється у комп’ютерах, мережах, автоматизованих системах, вчинені особою, яка має право доступу до такої інформації (ст. 362) [20].

Зазначені діяння є саме кримінальними правопорушеннями за умови, якщо вони вчинені належним суб’єктом, а також за низки інших умов (наприклад,

заподіяння шкоди відповідного характеру і обсягу). Зазначимо, що до інформаційних злочинів відносяться лише найнебезпечніші діяння у кіберпросторі, які не вичерпують усього спектру існуючих кіберзагроз [5].

В цілому, залежно від сфери (характеру) виникнення, загрози безпеки інформаційних систем поділяються на такі групи:

- природні;
- технічні;
- програмні (пов’язані із програмним забезпеченням);
- користувацькі.

Ця класифікація частково уже була розглянута вище у контексті напрямків превенції кіберзагроз підприємства. Прикладами природних загроз є повені, буревії, землетруси тощо. Їхнє значення як дестабілізуючих факторів кібербезпеки оцінюється з урахуванням повторюваності, частоти (за умови повторюваності) і рівня впливу (сили коливань, висоти води тощо). Ці показники варіюються залежно від розташування конкретного підприємства та. Меншою мірою, від інших чинників.

Технічні загрози кібербезпеки полягають у несправності чи пошкодженні устаткування (обладнання), яке є невід’ємною складовою інформаційній системі. Найчастіше технічні загрози мають механічний, електричний, термічний, рідше хімічний характер [25].

Варто зазначити, що класифікація загроз безпеки інформаційних систем залежно від сфери а також характеру їх виникнення є доволі умовною і, по суті, здійснюється за принципом першості впливу того чи іншого дестабілізуючого фактору. В подальшому, якщо реалізацію ризику не вдасться зупинити чи, принаймні, звести до мінімуму, вона обумовить ланцюгову реакцію.

Так, наприклад, така природна загроза, як повінь, може не лише тимчасово обмежити доступ до устаткування, але і спричинити короткі замикання, корозію тощо.

Програмні загрози кібербезпеки є найширшою групою, яка, з огляду на свою масштабність та динамічність, практично не піддається чіткому окресленню. Програмні загрози можуть бути пов’язані як із власним програмним забезпеченням інформаційної системи, так і з втручанням сторонніх програм. Загрози, не пов’язані із втручанням сторонніх програм (вони ж – внутрішньо-системні), можуть існувати під час нормального функціонування програмного забезпечення в інформаційній системі (внаслідок умислу чи недалекоглядності, помилки розробника), а можуть бути пов’язаними із збоєм, тобто порушенням нормального функціонування.

Сторонні програми проникають у інформаційну систему та порушують доступність, цілісність, захищеність інформації, можливість її цільового використання. Для загального позначення більшості шкідливих сторонніх програм прийнято використовувати поняття вірусів. Прикладами (різновидами) вірусів, зокрема, є бутові (завантажувальні) віруси, хробаки, троянські коні, кейлогери, перезаписуючі віруси та багато інших.

Користувацькі загрози безпеки інформаційних систем можна поділити на необережні діяння (наприклад, помилку) та умисні дії. Останні характеризуються чітким наміром особи щодо порушення конфіденційності, цілісності, доступності інформації та інших негативних наслідків для інформаційної системи.

Говорячи про запобігання ризикам кібербезпеки на конкретному підприємстві, необхідно з’ясувати уразливість його інформаційної системи до кіберзагроз. Уразливість інформаційної системи тлумачать як ознаку, яка характеризує наявність і масштабність (за наявності) недоліків та прогалин в устаткуванні і, перш за все, програмному забезпеченні інформаційної системи, а також супутніх обставин організаційного, управлінського, фізичного,

антропогенного та іншого характеру, які можуть як окремо, так і в комплексі обумовлювати реалізацію ризиків кібербезпеки або ж сприяти такій реалізації.

За критерієм уразливості інформаційної системи підприємства можуть визначатися як схильні або не схильні до загроз. Схильними до загроз є підприємства, інформаційні системи яких характеризуються високим рівнем уразливості, і навпаки. Суттєво, що показник уразливості об'єктивно не може бути нульовим, так як спектр кіберзагроз є занадто широким і мінливим.

Відповідно, доречно говорити не про наявність або відсутність уразливості інформаційної системи, а про її допустиме або ж недопустиме значення [32]. Підвищення уразливості інформаційної системи може бути обумовлено численними факторами, які самі по собі не обов'язково є негативними. Такими факторами є, наприклад, висока стандартизація устаткування і програмного забезпечення, зростання чисельності користувачів тощо. За змістом ризики кібербезпеки прийнято класифікувати наступним чином:

- ризики щодо конфіденційності інформації;
- ризики щодо цілісності інформації;
- ризики щодо доступності інформації.

Під конфіденційністю інформації розуміють установлений режим її розповсюдження. Цей режим включає:

- коло осіб, наділених доступом до даних (повністю або частково);
- обсяг повноважень окремих осіб щодо даних (ознайомлення, зміна, розповсюдження тощо);
- нормативні засади захисту інформації;

процедуру поширення інформації (випадки, обсяг, порядок тощо).

Конфіденційність та цілісність даних є тісно пов'язаними ознаками, які полягають у відсутності несанкціонованих змін обсягу, змісту, структури

послідовності, та форми викладу інформації, як в цілому, так і щодо її окремих частин.

Доступність даних – це характеристика, яка передбачає об'єктивну можливість санкціонованого доступу компетентних осіб до інформації та її цільового використання. Реалізація ризиків кібербезпеки підприємства обумовлює значні матеріальні втрати. Це може бути як заподіяння підприємству майнової шкоди у формі реальних збитків і втраченої вигоди, так і заподіяння моральної шкоди, зокрема, щодо ділової репутації. Збитки, завдані реалізацією ризиків безпеки інформаційної системи підприємства, можуть виражатися у формі пошкодження устаткування, програмного забезпечення, втрати даних тощо.

Завдана шкода полягає у тимчасовому повному або частковому блокуванні діяльності підприємства, внаслідок чого унеможливлюється укладення чи належне виконання вигідних договорів. Цьому слідує, як мінімум, втрата доходу, який міг би бути отриманим за звичайних обставин, а як максимум, претензійно-позовні формальності, ініційовані незадоволеними кредиторами.

Окрім того, у випадку реалізації кіберзагроз підприємство може бути притягнуто до юридичної відповідальності, передусім, цивільної та господарської, за порушення нормативно-правових та договірних засад захисту інформації.

Це стосується і персональних даних, якими володіє або розпоряджається суб'єкт господарювання, наприклад, персональних даних працівників, клієнтів тощо, і таємної, конфіденційної інформації, наприклад, щодо господарської діяльності договірних контрагентів (інших підприємств).

1.5 Управління ризиками у процесі обробки інформації

Говорячи про запобігання реалізації ризиків кібербезпеки підприємства, не можна оминути увагою поняття управління ризиками у процесі обробки

інформації. В цілому, під управлінням ризиками у менеджменті розуміють комплекс (систему) заходів, спрямованих на забезпечення мінімально можливих показників ризиків, які супроводжують функціонування бізнесу [33].

Ефективне управління ризиками кібербезпеки має важливе значення для безпеки підприємства загалом. Ризик-менеджмент є триваючою діяльністю, яка включає такі етапи:

- дослідження;
- визначення стратегії;
- вплив;
- контроль.

За загальним правилом, управління ризиками розпочинається із аналізу, який передбачає з'ясування сфери, типу, характеру існуючих загроз, оцінки їх ступеня та можливих наслідків впливу на діяльність підприємства у випадку реалізації. Саме це і становить зміст дослідження ризиків.

Еволюція методики управління ризиками кібербезпеки підприємства включає послідовність таких підходів:

- технічний;
- менеджерський;
- інституційний [13].

Технічний підхід зосереджений передусім на захисті окремих елементів інформаційної системи:

- апаратного устаткування;
- програмного забезпечення;
- даних.

Технічні методи зводяться, в цілому, до підготовки сценаріїв на випадок збою системи та резервного копіювання даних. Під резервним копіюванням

розуміють процес створення копії даних з носія, призначений для відновлення цих даних у разі їхнього пошкодження (зміни) чи втрати (видалення) [15].

Менеджерський підхід до управління ризиками кібербезпеки полягає у включенні безпеки інформаційної системи до комплексної політики безпеки підприємства. Такий підхід не виключає застосування технічних методів, проте значно ширшим, здатним забезпечувати не лише збереження інформації, але і її належну конфіденційність.

Інституційний підхід, що використовується для управління ризиками безпеки інформаційної системи, включає такі елементи:

- стандартизацію безпеки інформаційної системи;
- атестацію рішень щодо кібербезпеки;
- уніфікацію механізмів для вимірювання безпеки інформаційної системи на підприємстві.

Стандартизація передбачає запровадження у практику господарської діяльності високих вимог (стандартів) щодо безпеки інформаційної системи, а також механізмів забезпечення дотримання цих вимог. Атестація передбачає незалежну оцінку рішень щодо кібербезпеки, зокрема, їхнього коефіцієнта корисної дії (необхідності та ефективності відносно витрат). Уніфікація механізмів для вимірювання безпеки ІС забезпечує можливість ефективного моніторингу [6].

1.6 Організація інформаційної безпеки підприємства

На сьогоднішній день своєчасна та об’єктивна інформація є важливим фактором виробництва, який розглядають, як один з основних ресурсів розвитку суспільства. Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників.

Проте глобальна комп’ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави.

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб’єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій.

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

- протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення встановлених регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- помилки в проектуванні інформаційних систем;
- відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо.

Захист інформації – галузь науки і техніки, яка динамічно розвивається, пропонує ринку широкий спектр засобів для захисту даних. Проте жоден з них окремо взятий не може гарантувати адекватну безпеку інформаційної системи. Необхідною умовою ефективного захисту є проведення комплексу взаємодоповнюючих заходів.

Комплексне забезпечення інформаційної безпеки автоматизованих систем – це сукупність криптографічних, програмно-апаратних, технічних, правових, організаційних методів і засобів забезпечення захисту інформації при її обробці, зберіганні та передачі з використанням сучасних комп’ютерних технологій.

Фахівцями досліджується досить широкий перелік загроз безпеці інформаційних систем, які класифікують за рядом ознак (див. Рис 1.3.).

Рис 1.3. Класифікація загроз безпеці інформаційної системи

Досвід показує, що практично кожне підприємство має антивірусні засоби захисту, системи ідентифікації користувачів, системи управління доступом до інформаційної системи тощо. Тобто потенціал засобів захисту є, але він не реалізується фірмами повністю. Більше того, володіючи складними апаратними засобами захисту інформації, більшість підприємств навіть наполовину не використовують їх потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту.

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс

превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб.

Головними етапами побудови політики інформаційної безпеки є:

- реєстрація всіх ресурсів, які мають бути захищені;
- аналіз та створення переліку можливих загроз для кожного ресурсу;
- оцінка ймовірності появи кожної загрози;
- вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему.

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію).

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві:

- Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних;
- Підсистема управління контролем доступу та ідентифікацією в інформаційній системі;
- Підсистема міжмережевого екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережевих екранів;
- Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних;

- Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування;
- Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації;
- Підсистема захисту систем управління базами даних;
- Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму;
- Підсистема захисту мобільних пристроїв;
- Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них.

Спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування фірми.

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності.

Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Причому необхідна розробка концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов’язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту

входів-виходів мережі тощо), але і відповідні заходи адміністративного та технічного характеру.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами [26].

1.7 Теоретичні відомості про модель порушника

Порушник - це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо. Відносно АС порушники можуть бути внутрішніми (з числа персоналу або користувачів системи) або зовнішніми (сторонніми особами).

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ (далі – НСД) до роботи з включеними до складу ІТС засобами [4].

Модель порушника повинна визначати:

- можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;
- категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

По відношенню до автоматизованої системи порушники можуть бути внутрішніми або зовнішніми.

Зовнішніх порушників можна розділити на:

- добре озброєну та технічно оснащену групу, що діє зовні швидко і напролом;
- поодиноких порушників, що не мають допуску на об'єкт і намагаються діяти потайки й обережно, так як вони усвідомлюють, що сили реагування мають перед ним переваги.

Сторонні особи, що можуть бути порушниками:

- клієнти (представники організацій, громадяни);
- відвідувачі (запрошені з якого-небудь приводу);
- представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо);
- представники конкуруючих організацій (іноземних служб) або особи, що діють за їх завданням;

- особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку);
- будь-які особи за межами контрольованої зони.

Потенціальних внутрішніх порушників можна розділити на:

- допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєво важливого центру ІТС;
- основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);
- співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІТС, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Крім професійного шпигунства, можна виділити три основних мотиви порушень: безвідповідальність, самоствердження та корисливий інтерес.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки ІТС може бути викликано корисливим інтересом користувача ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для несанкціонованого доступу до інформації в ІТС.

Усіх порушників можна класифікувати за такими ознаками:

- за рівнем знань про ІТС;
- за рівнем можливостей;
- за часом дії;
- за місцем дії [4].

За рівнем знань про ІТС (в залежності від кваліфікації та професійної майстерності):

- володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС;
- володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування;
- володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС;
- знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості.

За рівнем можливостей (в залежності від методів і засобів, що використовуються):

- застосовує чисто агентурні методи отримання відомостей;
- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);
- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії інформації, які можуть бути тайком пронесені крізь пости охорони;
- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, перехоплення з каналів передачі даних, впровадження спеціальних програмних закладок).

За часом дії (в залежності від активності або пасивності системи):

- у процесі функціонування (під час роботи компонентів системи);
- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.);
- як у процесі функціонування, так і в період неактивності системи.

За місцем дії (в залежності від території доступу до засобів системи):

- без доступу на контрольовану територію організації;
- з контрольованої території без доступу до будівель та споруджень;
- усередині приміщень, але без доступу до технічних засобів;
- з робочих місць кінцевих користувачів (операторів);
- з доступом у зону даних (баз даних, архівів тощо);
- з доступом у зону управління засобами забезпечення безпеки.

Під час формування моделі порушника обов'язково повинно бути визначено:

- ймовірність реалізації загрози;
- своєчасність виявлення;
- відомості про порушення.

Слід зауважити, що всі злочини, зокрема і комп’ютерні, здійснюються людиною. Користувачі ІТС, з одного боку, є її складовою частиною, а з іншого – основною причиною і рухаючою силою порушень і злочинів. Отже, питання безпеки захищених ІТС фактично є питанням людських відносин та людської поведінки [4].

1.8 Реалізація моделі порушника

Метою порушника можуть бути отримання необхідної інформації у потрібному обсязі та асортименті (М1), мати можливість вносити зміни в інформаційні потоки (М2) та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей (М3).

За рівнем можливостей, що надаються їм засобами автоматизованої системи, порушники поділяються на тих, хто має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки

інформації (З1), тих, хто має можливість створення і запуску власних програм (З2) та тих, хто має можливість управління функціонуванням автоматизованої системи, впливу на базове програмне забезпечення системи і на склад і конфігурацію її устаткування (З3).

За рівнем знань про автоматизовані системи усіх порушників можна класифікувати як таких, що мають невисокий рівень знань інформаційних технологій, володіють інформацією про функціональні особливості автоматизованої системи (К1), тих, що володіють середнім рівнем знань інформаційних технологій, мають досвід роботи з технічними засобами автоматизованої системи та їхнього обслуговування (К2), тих, що володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації автоматизованої системи (К3) та тих, що володіють інформацією про функції та механізм дії засобів захисту (К4).

За місцем здійснення дії можуть класифікуватись на тих, хто не має доступ на контрольовану територію (Д1), тих, хто має доступ до КТ, але не має доступу до технічних засобів АС (Д2), на тих, хто має доступ до робочих місць кінцевих користувачів системи (Д3), та тих, хто має доступ до засобів адміністрування системи (Д4).

Порушники можуть діяти в робочий (Ч1) та в неробочий час (Ч2).

Для підприємства порушників можна розділити на наступні групи (дирекція підприємства, як розпорядник підприємства та за відсутності мети порушення у моделі не враховується):

- служба безпеки;
- адміністратор ІТС;
- користувач;
- технік ІТС;
- електрик;
- прибиральник.

Використовуючи наведені класифікації, була побудована модель порушника, наведена у табл. 1.1.

Рівні небезпеки порушника для підприємства визначені як вірогідність реалізації загрози цим порушником.

Таблиця 1.1

Модель внутрішнього порушника політики безпеки інформації						
Категорія порушника "ПБ"	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання захисту	Можливості за часом дії	Можливості за місцем дії	Рівень небезпеки
Служба безпеки	М1	К1	З1	Ч4	Д3	ВИСОКИЙ
Адміністратор ІТС	М1	К4	З1	Ч4	Д4	ВИСОКИЙ
Користувач	М1	К2	З1	Ч3	Д2	СЕРЕДНІЙ
Технік ІТС	М1	К2	З1	Ч4	Д3	СЕРЕДНІЙ
Електрик	М1	К1	З1	Ч1	Д1	НИЗЬКИЙ
Прибиральник	М1	К1	З1	Ч4	Д1	НИЗЬКИЙ

З таблиці видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС та служба безпеки. Тому організація роботи цього персоналу повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

Висновки до першого розділу

Отже, у сучасних умовах інформаційна безпека є невід’ємною складовою системи безпеки будь якого підприємства. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення і нейтралізацію тих обставин, факторів і дій, які можуть задати збиток.

Варто розуміти, що розробка стратегії управління ризиками не замінює прийняття рішень при безпосередньому впливі на ризики. Метою впливу є приведення показників існуючих ризиків до їхніх мінімально можливих значень, відповідно до умов.

Було розглянуто та розроблено модель порушника яка показала, що розробка адекватної та максимально описаної моделі порушника є обов’язковим етапом побудови надійної системи інформаційної безпеки на підприємстві, що дасть змогу попередити її знищення, модифікацію чи підміну.

Сутність викладеного дає підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства неможливо забезпечити його надійну безпеку та розвиток.

Розділ 2

МЕТОДИ ТЕСТУВАННЯ ТА АНАЛІЗУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Надійність програмного забезпечення інформаційних систем

Розвиток інформаційних технологій та комп’ютерної техніки та всебічне проникнення її в усі сфери життєдіяльності людини передбачає постановку нових задач для розробників програмного забезпечення. Програмні продукти стають дедалі складнішими, багатокомпонентними і вимагають спеціалізованого підходу.

За умови досягнення високої надійності, сучасна техніка стає ефективною та конкурентоспроможною. Саме від показника надійності похідними будуть інші, не менш важливі показники – якість, живучість, безпека, готовність.

В багатьох дослідженнях поняття надійності програмного забезпечення (ПЗ) виділяють окремо, тому, що при застосуванні понять надійності до програмних засобів варто враховувати особливості і відмінності цих об'єктів від традиційних технічних систем, для яких спочатку розроблялася теорія надійності. Принципова відмінність програм від техніки, та технічних систем зокрема, полягає в тому, що програма не зношується з плином часу, а навпаки, виявляються помилки, які не були знайдені раніше, ПЗ з часом вдосконалюється і покращується.

Водночас підвищуються і вимоги до надійності та витривалості програм, виникає потреба у скороченні затрат на тестування та, відповідно, у прогнозуванні надійності розроблюваного програмного забезпечення.

Для розв’язання таких задач оцінки та прогнозування надійності на даний час використовують моделі надійності. Однак, усі моделі містять цілий ряд

спрощень і припущень, що зменшує клас задач та область застосування їх для реального об'єкту.

Тому, на сьогодні актуальною задачею програмної інженерії є розроблення моделей надійності ПЗ з підвищеним ступенем адекватності реальним об’єктам.

Модель надійності програмного забезпечення передбачає побудову математичної моделі для оцінки залежності надійності програмного забезпечення від певних параметрів. На рис. 2.1. виділено моделі, які кількісно оцінюють показники надійності на етапі експлуатації комп’ютерних систем. Зокрема, параметрами, що пов'язані з деякою гілкою програми на підмножині наборів вхідних даних, за допомогою яких ця гілка контролюється.

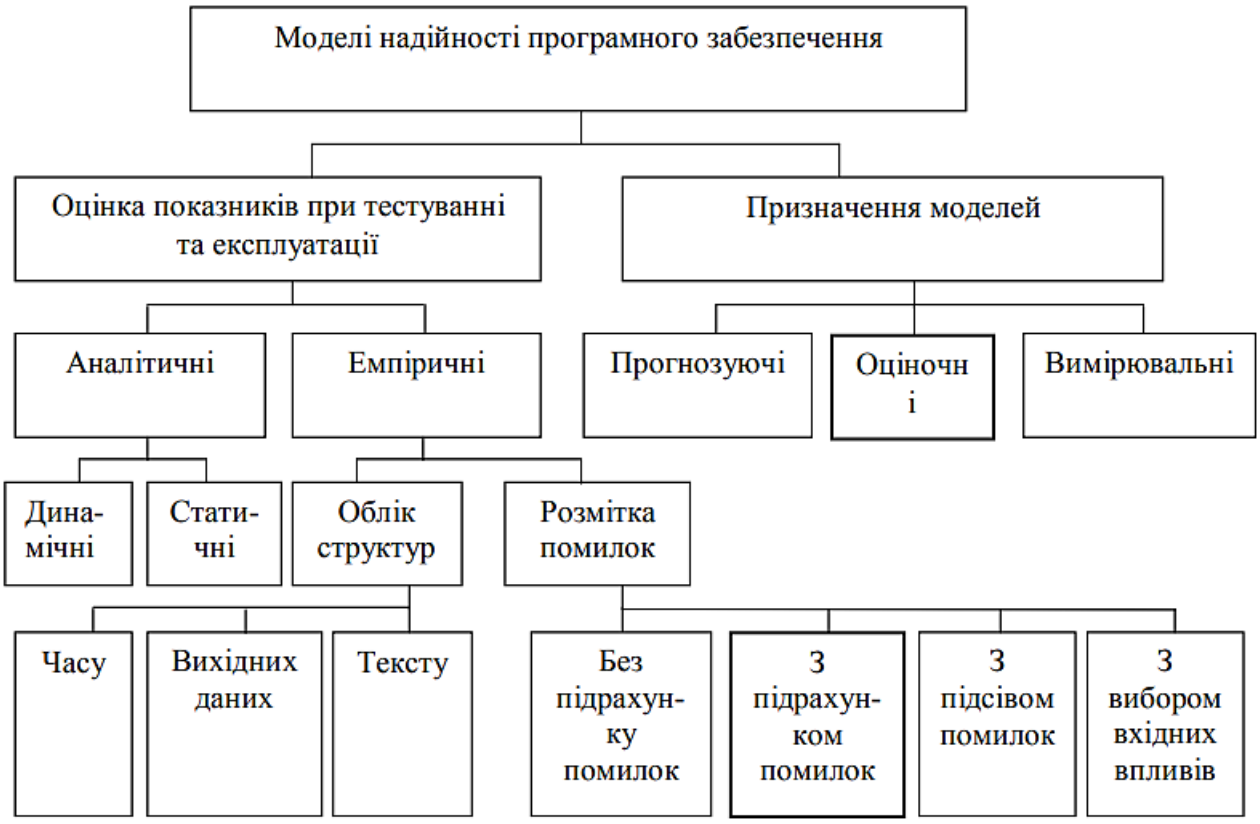

Рис. 2.1. Види моделей надійності програмного забезпечення

Іншими такими параметрами є частота помилок, які дозволяють оцінити якість систем реального часу, що функціонують в безперервному режимі, і в той

же час отримувати непряму інформацію про надійність ПЗ. Виділяють чотири типи моделей надійності:

- аналітичні;
- динамічні;
- статичні;
- емпіричні.

Найбільш широко використовуються динамічні моделі на основі неоднорідного Пуассонового процесу, в яких вихідні дані збираються в процесі тестування ПЗ протягом фіксованих або випадкових часових інтервалів.

Кожен інтервал – це стадія на якій виконується послідовність тестів і виявляється деяка кількість помилок [41].

2.2 Експоненціальна модель Шумана

Дана модель базується на наступних припущеннях:

– загальне число команд у програмі на машинній мові постійне;

– на початку випробувань число помилок дорівнює деякій постійній величині та по мірі виправлення помилок стає меншим; у ході виправлення програми нові помилки не вносяться;

– інтенсивність відмов програми пропорційна числу залишкових помилок.

Про структуру програмного модуля зроблені наступні припущення:

– модуль містить тільки один оператор циклу, в якому є оператори вводу інформації, оператори присвоєння та оператори умовної передачі управління вперед;

– відсутні вкладені цикли, але може бути *k* паралельних шляхів, якщо маємо *k* –1 оператор умовної передачі управління. [14]

При виконанні зазначених припущень ймовірність безвідмовної роботи знаходять за формулою:

$$R(t,\tau)=\exp(-C\varepsilon_r(\tau)t)=e^{-t/T};\ \varepsilon_r(\tau)=\frac{E_0}{I}-\varepsilon_B(\tau);\ T=\frac{1}{\left(C\left(\frac{E_0}{I}-\varepsilon_B(\tau)\right)\right)} \quad , (2.1)$$

де E_0 – число помилок на початку налагодження; I – число машинних команд у модулі; $\varepsilon_B(\tau)$, $\varepsilon_r(\tau)$ – число виправлених і залишених помилок у розрахунку на одну команду; T – середній наробіток на відмову; τ – час налагодження; C – коефіцієнт пропорційності.

Для оцінки E_0 і C використовують результати налагодження. Нехай із загального числа прогонів системних тестових програм r – число успішних прогонів, $n-r$ – число прогонів, що перервані помилками. Тоді загальний час n прогонів, інтенсивність помилок і наробіток на помилку знаходять за формулами

$$H=\sum_{i=1}^{r}T_i+\sum_{i=1}^{n-r}t_i;\ \lambda=\frac{n-r}{H};\ T=\frac{1}{\lambda}=\frac{H}{n-r} \quad , (2.2)$$

Припустивши, що $H=\tau_i$ і $H=\tau_2$, знайдемо:

$$\tilde{\lambda}_1=\frac{n_1-r_1}{H_1};\ \tilde{\lambda}_2=\frac{n_2-r_2}{H_2};\ \tilde{T}_1=\frac{1}{\tilde{\lambda}_1};\ \tilde{T}_2=\frac{1}{\tilde{\lambda}_2} \quad , (2.3)$$

де T_1 і T_2 – час тестування на одну помилку. Підставивши сюди (2.1) та розв'язавши систему рівнянь, отримаємо оцінки параметрів моделі:

$$\tilde{E}_0 = \frac{I}{\gamma - 1}\left(\gamma\varepsilon_B(\tau_1) - \varepsilon_B(\tau_2)\right);\ \tilde{C} = \frac{1}{\left(\tilde{T}_1\left(\frac{\tilde{E}_0}{I} - \varepsilon_B(\tau_1)\right)\right)};\ \gamma = \frac{\tilde{T}_1}{\tilde{T}_2} \quad , (2.4)$$

Для обчислення оцінок необхідно по результатам налагодження знати T_1 , T_2 , $\varepsilon_B(\tau_1)$, $\varepsilon_B(\tau_2)$.

Деяке узагальнення результатів (2.2) – (2.4) полягає в наступному. Нехай T_1 і T_2 – час роботи системи, що відповідає часу налагодження τ_1 і τ_2 , n_1 і n_2 – число помилок, виявлених у періодах τ_i і τ_2. Тоді:

$$\frac{T_1}{n_1} = \frac{1}{\left(C\left(\frac{E_0}{I} - \varepsilon_B(\tau_1)\right)\right)},\ \frac{T_2}{n_2} = \frac{1}{\left(C\left(\frac{E_0}{I} - \varepsilon_B(\tau_2)\right)\right)}$$

Звідси:

$$\tilde{E}_0 = \frac{I}{\gamma - 1}\left(\gamma\varepsilon_B(\tau_1) - \varepsilon_B(\tau_2)\right);\ \tilde{C} = \frac{\frac{n_1}{T_1}}{\left(\frac{\tilde{E}_0}{I} - \varepsilon_B(\tau_1)\right)};\ \gamma = \frac{T_1}{n_1}\Big/\frac{T_2}{n_2}. \quad , (2.5)$$

Якщо T_1 і T_2 – лише сумарний час налагодження, то $\tilde{T}_1 = T_1/n_1$, $\tilde{T}_2 = T_2/n_2$, то формула (2.5) співпадає з (2.4).

Якщо в ході налагодження проводиться k тестів в інтервалах $(0,\tau_1)$, $(0,\tau_2)$,... $(0,\tau_k)$, *де* $\tau_1 < \tau_2 < \ldots < \tau_k$, то для визначення оцінок максимальної правдоподібності використовують рівняння:

$$\tilde{C} = \sum_{j=1}^{k} n_j \Big/ \left(\frac{\tilde{E}_0}{I} - \varepsilon_B(\tau_j) \right) H_j ; \; \tilde{C} = \left\{ \sum_{j=1}^{k} n_j \Big/ \left(\frac{\tilde{E}_0}{I} - \varepsilon_B(\tau_j) \right) \right\} \sum_{j=1}^{k} H_j \quad , (2.6)$$

де n_j – число прогонів j -го тесту, що закінчуються відмовами; H_j – час, що затрачається на виконання успішних і неуспішних прогонів j -го тесту. При $k = 2$ (2.6) зводиться до попереднього випадку і розв'язок дає результат (2.5).

Асимптотичне значення дисперсій оцінок (для великих значень n_j) визначаються виразами:

$$D\tilde{C} = 1 \Big/ \left\{ \sum_{j=1}^{k} n_j \Big/ C^2 - \left(\sum_{j=1}^{k} H_j \right)^2 \Big/ \sum_{j=1}^{k} \left(n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right)^2 \right) \right\}$$

$$DE_0 = 1 \Big/ \sum_{j=1}^{k} \left\{ \left(n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right)^2 \right) - C^2 \left(\sum_{j=1}^{k} H_j \right)^2 \Big/ \sum_{j=1}^{k} n_j \right\}$$

де $C \cong C$, $E_0 \cong E_0$.

Коефіцієнт кореляції оцінок:

$$\rho(C,E) \cong \left\{ \sum_{j=1}^{k} n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right) \right\} \Big/ \left\{ \sum_{j=1}^{k} n_j \sum_{j=1}^{k} \left(n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right)^2 \right) \right\}^{0,5}$$

Асимптотичне значення дисперсії і коефіцієнта кореляції використовуються для визначення довірчих інтервалів значень E_0 і C на основі гаусівського розподілу.

У ряді робіт зазначається, що найбільш адекватною для моделі Шумана є експоненціальна модель зміни кількості помилок при зміні тривалості налагодження $\varepsilon_B(\tau) = \frac{E_0}{I}\left(1 - e^{-\tau/\tau_0}\right)$, де E_0 і τ_0 визначаються дослідним шляхом. Тоді $R(t,\tau) = \exp\left(-CE_0 / Ie^{-I/I_0}t\right)$. Середній наробіток на відмову зростає експоненціально зі збільшенням тривалості налагодження: $T = I \Big/ CE_0 e^{\frac{\tau}{\tau_0}}$. [40]

2.3 Експоненціальна модель Джелінські-Моранді

Дана модель є частинним випадком моделі Шумана. Згідно цієї моделі, інтенсивність появи помилок пропорційна числу залишкових помилок:

$\lambda(\Delta t_i) = K_{JM}(E_0 - i+1)$, де K_{JM} – коефіцієнт пропорційності; Δt_i – інтервал між i -ю та $(i-1)$-ю виявленими помилками. Ймовірність безвідмовної роботи

$$R(t) = \exp(-\lambda(\Delta t)) = \exp(-K_{JM}(E_0 - i + 1)),\ t_{i-1} < t < t_i \qquad (2.7)$$

При $K_{JM} = C/I$ і $\varepsilon_B(\tau) = (i-1)/I$ формула (2.7) співпадає з (2.1). Для того щоб отримати оцінки максимальної правдоподібності для параметрів E_0 і τ_0 при послідовному спостереженні k помилок у моменти $t_1, t_2, \ldots, t_k$, потрібно розв'язати систему рівнянь:

$$\sum_{i=1}^{k}\left(E_0 - i + 1\right)^{-1} = k \Big/ \left(E_0 - i + 1\right);\quad K_{JM} = \frac{k}{A} \Big/ \left(E_0 - \theta \cdot k + 1\right)$$

$$\theta = \frac{B}{AK};\ A = \sum_{i=1}^{k} t_i;\ B = \sum_{i=1}^{k} it_i$$

Асимптотичні оцінки дисперсії і коефіцієнта кореляція (при великих) k визначаються за допомогою формул:

$$DE_0 \cong \frac{k}{kS_2 - A^2C^2};\ DK_{JM} \cong \frac{S_2K_{JM}^2}{kS_2 - A^2K_{JM}^2}$$

$$\rho\left(K_{JM}, E_0\right) \cong \frac{AK_{JM}}{\left(kS_2\right)^{0,5}};\ S_2 = \sum_{i=1}^{k}\left(E_0 - i + 1\right)$$

Для того щоб отримати числові значення цих величин, необхідно скрізь замінити E_0 і K_{LM} їх оцінками [14].

2.4 Структурна модель Нельсона

Модель, що отримала назву модель Нельсона (Nelson), є біноміальною моделлю Бернуллі з накладеними правилами щодо використання вхідних даних. Зокрема, область вхідних даних Пз задається у вигляді k непересічних областей - $\{Z_i\}$, яким однозначно відповідає безліч ймовірностей $\{p_i\}$, тому що відповідний набір даних буде обраний для чергового прогону ПЗ.

Таким чином, якщо при виконанні прогонів програми (на Z_i наборі вхідних даних)n_i з них закінчилися відмовою, то ступінь надійності функціонування ПО визначається виразом:

$$P = 1 - \sum_{i=1}^{k} \frac{n_i}{N_i} p_i \quad , (2.8)$$

Модель дозволяє розрахувати ймовірність P_u безвідмовного виконання програми n-прогонів програми:

$$P_u = \prod_{j=1}^{u}(1 - Q_j) = e^{\left(\sum_{j=1}^{u} \ln(1-Q_j)\right)} \quad , (2.9)$$

Де: $Q_j = \sum_{i=1}^{k} p_{ji}\chi_i$, χ_I - характеристична функція відмови на i-му наборі даних; ρ_{ji} - ймовірність появи i-го набору в j-му прогоні.

У структурній модифікації моделі Нельсона пропонується для знаходження використовувати аналіз графа ПЗ. На жаль, проведення аналізу структурно-складної модифікації ПЗ для вирішення зазначених завдань на практиці не представляється ефективним.

До недоліків моделі також відносять вимоги по великій кількості випробувань для отримання точних оцінок. Однак дана категорія труднощів вирішується шляхом застосування статистичного методу Вальда. Можна продемонструвати перехід від моделей налагодження до тимчасових моделей.

Вважаючи, що Δt_j - час виконання j-го прогону, можна отримати наступний розрахунковий вираз:

$$P_u = e^{(\sum_{j=1}^{u} \lambda(t_j)\Delta t_j)} \quad , (2.10)$$

Де: $\lambda(t_j) = \frac{-\ln(1-Q_j)}{\Delta t_j}$ - інтенсивність відмови,

$t_j = \sum_{i=1}^{j} \Delta t_i)$ - сумарний час виконання j-прогонів ПЗ.

Вважаючи, що Δt_j стає відносно малою величиною зі зростанням u-числа випробувань, маємо:

$$P(t) = e^{-\int_0^t \lambda(z)dz} \quad , (2.11)$$

2.5 Розрахунок числа відмов програмного забезпечення

На сьогодні відсутня єдина теорія, адекватно відображаюча надійність ПЗ, так як всі відомі моделі одностороннє розглядають процес появи програмних помилок.

Встановлено, що процес виявлення помилки в ПЗ практично є перехідним процесом в лінійній системі першого порядку, що відкриває нові можливості в дослідженні та уточненні моделей надійності ПЗ.

На основі дослідження реальних статистичних даних по надійності ПЗ в табл. 2.1 показані результати розрахунку значень дисперсії *(D)* і середнього квадратичного відхилення *(σ)* прогнозованого *(m_i)* від експериментального *(m_i^*)* числа відмов ПЗ за *i* - місяців експлуатації комп'ютерної системи *(i =1,12)*.

$$D = \frac{1}{T}\sum_{i=1}^{T}(m_i^* - m_i)^2; \quad \sigma = \sqrt{D}\,; \quad T = 12;$$

Таблиця 2.1.

Ранг	Моделі надійності програмного забезпечення	$\sum_i^T (m_i^*\text{-}m_i)$	D	σ
1	Модель перехідного процесу	13,37	1,114	1,056
2	Експоненціальна модель Шумана	13,91	1,159	1,077
3	Проста експоненціальна модель	13,93	1,161	1,077
4	Модель Джелінські - Моранді	17,15	1,429	1,195
5	Модель S - образного зростання надійності	43,97	4,752	3,18
6	Модель Вейбулла	64,86	5,405	2,325
7	Геометрична модель Моранді	71,2	5,993	2,436

Аналіз отриманих результатів показує, що з урахуванням доступності вхідних даних, обмежень і допущень, що відповідають реальним умовам експлуатації комп'ютерних систем, достатню для практики точність забезпечує модель Джелінскі-Моранді (m_i' на рис. 2.2), при цьому в кращу сторону виділяється модель перехідних процесів (m_i'' на рис. 2.2), а в гіршу – геометрична Моранді (m_i''' на рис. 2.2).

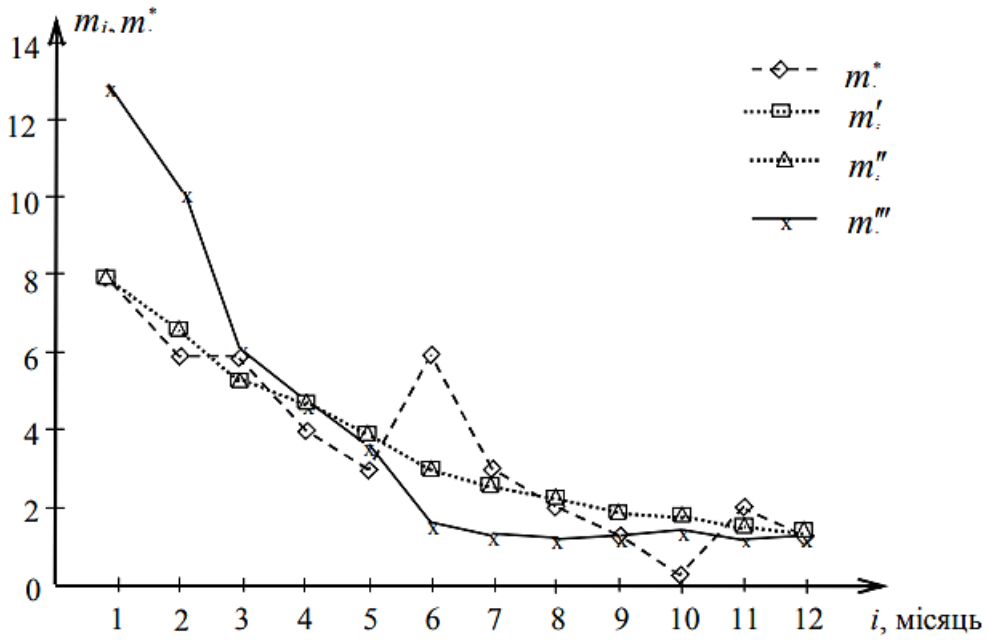

Рис. 2.2. Залежності істинного і прогнозованого числа відмов програмного забезпечення за рік експлуатації комп’ютерної системи

Залежності експериментальних даних (m_i^*) і результатів розрахунків з використанням моделі Джелінскі-Моранді (m_i) за рік експлуатації комп'ютерної системи показані на рис. 2.2.

Прояви помилок ПЗ в моделі Джелінскі-Моранді розглядаються як марковський процес, при цьому розподіл інтенсивності відмов експоненціальний, що добре погодиться з експериментальними даними. Допущення при використанні цієї моделі:

- інтенсивність виявлення помилок пропорційна поточному числу помилок в ПЗ;

- усі помилки однаково ймовірні й їх поява незалежна одна від іншої;
- поява кожної помилки приводить до порушення правильності функціонування ПЗ;
- час до наступного відказу ПЗ розподілено експоненціальний;
- ПЗ функціонує у середовищі близькому до реальних умов експлуатації комп’ютерних систем;
- помилки ПЗ після виявлення усуваються без внесення нових;
- інтенсивність виявлення помилок постійна в інтервалі між двома суміжними моментами появи помилок;
- після виявлення і усунення усіх помилок ПЗ надійність комп'ютерної системи визначається показниками АЗ.

На основі використання моделі надійності ПЗ Джелінскі-Моранді запропоновано методику, що дозволяє в реальних умовах експлуатації програмно-керованих засобів зв'язку оцінити показники надійності окремих складових і систем в цілому. По мірі накопичення статистичних даних про відмови ПЗ точність прогнозування результатів підвищується [34].

Висновки до другого розділу

Аналізуючи матеріал викладений у другому розділі можна зробити висновок, що будь-яке програмне забезпечення яке розробляється для тих чи інших задач повинне пройти тестування на надійність. Адже в сучасному світі програмні продукти стають дедалі складнішими, багатокомпонентними і вимагають спеціалізованого підходу.

Але потрібно розуміти що надійність програмного забезпечення не повинне ускладнювати його використання. Тому, на сьогодні актуальною задачею програмної інженерії є розроблення моделей надійності ПЗ з підвищеним ступенем адекватності до реальних об’єктів.

Розділ 3

ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

3.1 Загальні принципи побудови системи безпеки підприємства

Основою побудови ефективної системи інформаційної безпеки підприємства є забезпечення зв’язків (взаємодії) між усіма елементами та ресурсами цієї системи. В основному в якості ресурсів виступають комп’ютери, інша техніка, програмне забезпечення, інформаційні дані. В якості ж елементів виступають мережі зв’язків між цими ресурсами.

Як правило, створенню служби безпеки підприємства передують дві події:

- гостре бажання керівників підприємства відреагувати на раптово виниклі реальні загрози майну, фізичного проникнення, викрадення інформації і т.д.;
- заснований на результатах аудиту висновок про незадовільний стан безпеки підприємства.

Після детального вивчення стану безпеки підприємства (із залученням фахівців, якщо їх немає на підприємстві) у його керівників з’явиться реальне уявлення про систему безпеки підприємства. Таке системне уявлення (зафіксоване в письмовій формі) дозволяє усвідомлено і цілеспрямовано проводити роботу щодо забезпечення безпеки діяльності підприємства всіма його підрозділами й співробітниками. При цьому провідна роль служби безпеки не зникає, а навпаки, розуміння своєї ролі і місця в системі безпеки підприємства призведе тільки до позитивних результатів.

Для організації надійної системи захисту потрібно розуміти що головними структурними елементами захисту системи безпеки підприємства є:

- наукова теорія безпеки підприємства;
- політика і стратегія безпеки;
- засоби та методи забезпечення безпеки;
- концепція безпеки підприємства.

Система безпеки підприємства може бути побудована на основі наступних принципів:

1) Пріоритет заходів попередження. Зміст цього принципу передбачає своєчасне виявлення тенденцій і передумов, що сприяють розвитку загроз, на основі аналізу яких виробляються відповідні профілактичні заходи щодо недопущення виникнення реальних загроз.

2) Законність. Заходи безпеки підприємства розробляються на основі і в рамках чинних правових актів. Локальні правові акти підприємства не повинні суперечити законам і підзаконним актам.

3) Комплексне використання сил і засобів. Для забезпечення безпеки використовуються всі наявні в розпорядженні підприємства сили та засоби. Кожен співробітник повинен в рамках своєї компетенції брати участь у забезпеченні безпеки підприємства. Організаційною формою комплексного використання сил і засобів є програма забезпечення безпеки підприємства.

4) Координація та взаємодія всередині і поза підприємством. Заходи протидії загрозам здійснюються на основі взаємодії та скоординованості зусиль всіх підрозділів, служб підприємства, а також встановлення необхідних контактів із зовнішніми організаціями, здатними надати необхідне сприяння в забезпеченні безпеки підприємства.

5) Поєднання гласності з конспірацією. Доведення до відома персоналу підприємства та громадськості в допустимих межах заходів безпеки виконує

найважливішу роль – запобігання потенційних і реальних загроз. Така гласність, однак, повинна неодмінно доповнюватися в виправданих випадках заходами конспіративного характеру.

6) Компетентність. Співробітники та групи співробітників повинні вирішувати питання забезпечення безпеки на професійному рівні, а в необхідних випадках – спеціалізуватися по основних його напрямках.

7) Економічна доцільність. Вартість фінансових витрат на забезпечення безпеки не повинна перевищувати той оптимальний рівень, при якому втрачається економічний сенс їх застосування.

8) Планова основа діяльності. Діяльність по забезпеченню безпеки повинна будуватися на основі комплексної програми забезпечення безпеки підприємства, підпрограм забезпечення безпеки по основних його видах (економічна, науково-технічна, екологічна, технологічна і т.д.) і розроблюваних для їх виконання планів роботи підрозділів підприємства та окремих співробітників.

9) Системність. Цей принцип передбачає врахування всіх факторів, що впливають на безпеку підприємства, включення в діяльність щодо його забезпечення всіх співробітників підрозділів, використання в цій діяльності всіх сил і засобів.

Надійність і ефективність системи безпеки підприємства оцінюється на основі одного критерію – ступеня відсутності або наявності завданої йому матеріальної та моральної шкоди. Зміст цього критерію розкривається через ряд показників:

1) недопущення фактів витоку конфіденційних відомостей;

2) попередження або припинення протиправних дій з боку персоналу підприємства, його відвідувачів, клієнтів;

3) збереження майна та інтелектуальної власності підприємства;

4) попередження надзвичайних ситуацій;

5) припинення насильницьких злочинів відносно окремих (спеціально виділених) співробітників і груп співробітників підприємства;

6) своєчасне виявлення і припинення спроб несанкціонованого проникнення на охоронювані об’єкти підприємства.

Важливим елементом системи є оформлення технічної документації, якою керуватимуться всі працівники підприємства під час роботи. По суті вона регулюватиме 2 основні моменти: управлятиме доступом до інформації, та управлятиме потоками всієї інформації.

В загальному вигляді ця технічна документація врегулює функції захисту інформації, закріпить основоположні принципи побудови системи безпеки, забезпечить детальний опис процедур роботи з інформацією та порядок дій в надзвичайних ситуаціях.

Керівнику компанії необхідно буде, з одного боку, забезпечити ознайомлення всіх працівників з інформацією, що стосується забезпечення інформаційної безпеки, а з іншого – своєчасне внесення змін до документації, що може бути викликане об’єктивними чинниками (наприклад – появою нових ризиків) [14].

3.2 Політика і стратегія безпеки та її основи

Політика безпеки підприємства – це загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цілей. Т.ч., для встановлення цих загальних орієнтирів необхідно спочатку сформулювати цілі забезпечення безпеки підприємства. Такими цілями можуть бути:

- зміцнення дисципліни праці і підвищення його продуктивності;

- захист законних прав та інтересів підприємства;
- зміцнення інтелектуального потенціалу підприємства;
- збереження та примноження власності;
- підвищення конкурентоспроможності виробленої продукції;
- максимально повне інформаційне забезпечення діяльності підприємства і підвищення його ефективності;
- орієнтація на світові стандарти і лідерство в розробці та освоєнні нових технологій; – виконання виробничих програм;
- надання сприяння управлінським структурам у досягненні цілей підприємства;
- недопущення залежності від випадкових і несумлінних ділових партнерів.

З урахуванням вищевикладеного можна визначити наступні загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цих цілей:

- збереження і нарощування ресурсного потенціалу;
- проведення комплексу превентивних заходів щодо підвищення рівня захищеності власності і персоналу підприємства;
- включення в діяльність по забезпеченню безпеки підприємства всіх його співробітників;
- професіоналізм і спеціалізація персоналу підприємства;
- пріоритетність несилових методів запобігання і нейтралізації загроз.

Для успішного виконання цієї політики необхідно реалізувати стратегію безпеки підприємства, під якою розуміється сукупність найбільш значущих рішень, спрямованих на забезпечення прийнятного рівня безпеки функціонування підприємства. Виділяються такі типи стратегій безпеки:

1) орієнтовані на усунення існуючих або запобігання виникнення можливих загроз;

2) націлені на запобігання впливу існуючих або можливих загроз на предмет безпеки;

3) спрямовані на відновлення (компенсацію) завданої шкоди.

Перші два типи стратегій передбачають таку діяльність із забезпечення безпеки, в результаті якої не виникає загрози або створюється заслін її впливу. У третьому випадку збиток допускається (виникає), проте він компенсується діями, які передбачає відповідна стратегія.

Цілком очевидно, що стратегії третього типу можуть розроблятися і реалізовуватися стосовно ситуацій, де збитки можуть бути компенсовані, або тоді, коли немає можливості здійснити будь-яку програму реалізації стратегій першого або другого типу [14].

3.2.1 Суб’єкти та об’єкти безпеки підприємства

У кожній державі об’єктами інформаційної безпеки виступають передусім люди (усі громадяни) і держава, як цілісність, а основним каналом інформаційного впливу завжди є свідомість, психіка людини, свідомість (переконання, утвердження і т. ін.) великого етносу [7].

Забезпеченням безпеки підприємства займаються дві групи суб’єктів. Перша група займається цією діяльністю безпосередньо на підприємстві і підпорядкована його керівництву. Серед цієї групи виділяють спеціалізовані суб’єкти (рада або комітет безпеки підприємства, служба безпеки, пожежна частина, рятувальна служба і т.д.), основним призначенням яких є постійна професійна діяльність щодо забезпечення безпеки підприємства (у рамках своєї компетенції).

Іншу частину суб'єктів цієї групи умовно можна назвати напівспеціалізованою, так як частина функцій цих суб'єктів призначена для забезпечення безпеки підприємства (медична частина, юридичний відділ і т.д.).

До третьої частини цієї групи суб'єктів належить увесь інший персонал і підрозділи підприємства, які в рамках своїх посадових інструкцій і положень про підрозділи зобов'язані вживати заходів до забезпечення безпеки. Слід мати на увазі, що ефективно забезпечувати безпеку підприємства ці суб'єкти можуть тільки в тому випадку, якщо цілі, завдання, функції, права і обов'язки будуть розподілені між ними в т.ч., щоб вони не перетиналися один з одним.

До другої групи суб'єктів відносяться зовнішні органи та організації, які функціонують самостійно і не підкоряються керівництву підприємства, але при цьому їх діяльність має суттєвий (позитивний чи негативний) вплив на безпеку підприємства. Суб'єктами цієї групи є:

- законодавчі органи;
- органи виконавчої влади;
- суди;
- правоохоронні органи;
- науково-освітні установи.

Останні (особливо недержавні установи з підготовки приватних охоронців) покликані забезпечити науково-методичне опрацювання проблем безпеки підприємства та підготовку відповідних фахівців у сфері безпеки підприємств.

Очевидно, що суб'єкти другої групи за своєю ініціативою підключаються епізодично (або ніколи) до діяльності підприємства із забезпечення своєї безпеки. Організаційною формою такого підключення може стати комплексна програма безпеки підприємства, в якій необхідно передбачити форми і методи цієї роботи. Крім того, можна рекомендувати розробку планів структурних підрозділів і всього підприємства в цілому по організації взаємодії з вищевказаними органами та організаціями [14].

3.2.2 Засоби та методи забезпечення безпеки підприємства

Найбільш популярними засобами забезпечення безпеки підприємства є:

1) Технічні засоби. До них відносяться охоронно-пожежні системи, відео-радіоапаратура, засоби виявлення вибухових пристроїв, бронежилети, загородження і т.д.;

2) Організаційні засоби. Створення спеціалізованих оргструктурних формувань, що забезпечують безпеку підприємства;

3) Інформаційні засоби. Насамперед, це друкована та відеопродукція з питань збереження конфіденційної інформації. Крім цього, найважливіша інформація для прийняття рішень з питань безпеки зберігається в комп'ютерах;

4) Фінансові кошти. Цілком очевидно, що без достатніх фінансових коштів неможливе функціонування системи безпеки: питання лише в тому, щоб використовувати їх цілеспрямовано і з високою віддачою;

5) Правові засоби. Тут мається на увазі використання не тільки виданих вищими органами влади законів і підзаконних актів, але й розробка власних, так званих локальних правових актів з питань забезпечення безпеки;

6) Кадрові кошти. Мається на увазі насамперед достатність кадрів, що займаються питаннями забезпечення безпеки. Одночасно з цим вирішують завдання підвищення їх професійної майстерності в цій сфері діяльності;

7) Інтелектуальні засоби. Залучення до роботи висококласних фахівців, науковців (іноді доцільно залучати їх з боку) дозволяє впроваджувати нові системи безпеки.

Слід зазначити, що застосування кожного з вищевказаних засобів окремо не дає необхідного ефекту: він можливий тільки на комплексній основі. У той же час

необхідно відзначити, що одночасне використання всіх вищевказаних коштів в принципі неможливо. Воно проходить зазвичай ряд етапів:

- виділення фінансових коштів;
- формування кадрових і організаційних засобів;
- розробка системи правових засобів;
- залучення технічних, інформаційних та інтелектуальних засобів.

Перекладені з статичного в динамічний стан вищевказані кошти стають методами, тобто прийомами, способами дії. Відповідно, можна говорити про технічні, організаційні, інформаційні, фінансові, правові, кадрові та інтелектуальні методи. Наведемо короткий конкретний перелік цих методів:

- технічні – спостереження, контроль, ідентифікація і т.д.;
- організаційні – створення зон безпеки, режим, розслідування, пости, патрулі і т.д.;
- інформаційні – складання характеристик на співробітників, аналітичні матеріали конфіденційного характеру тощо;
- фінансові – матеріальне стимулювання співробітників, що мають досягнення в забезпеченні безпеки, грошове заохочення інформаторів і т.д.;
- правові – судовий захист законних прав та інтересів, сприяння правоохоронним органам і т.д.;
- кадрові – підбір, розстановка і навчання кадрів, які забезпечують безпеку підприємства, їх виховання і т.д.;
- інтелектуальні – патентування, ноу-хау і т.д [15].

3.2.3 Концепція безпеки підприємства

Після вивчення всіх вищеописаних елементів системи безпеки підприємства необхідно перейти до складання й концепції.

Концепція визначається як система поглядів, ідей, цільових установок, пронизаних єдиним, визначальним задумом, провідною думкою, що містить постановку і шляхи вирішення виявлених проблем.

В подальшому під поняттям «концепція» розумітимемо концепцію предметної області досліджень, тобто концепцію безпеки підприємства. До будь-якої концепції можна встановити такі вимоги:

- Конструктивність. Така вимога буде визнана реалізованою, якщо в концепції знаходять відображення:

– початковий стан об’єкта, на перетворення якого спрямована концепція; – стан об’єкта, досягнутий в результаті реалізації концепції;

– заходи, необхідні для досягнення сформульованих у концепції цілей;

– кошти, необхідні і достатні для досягнення поставлених цілей;

– джерела ресурсного забезпечення, що використовуються в ході реалізації концепції;

– механізм реалізації концепції, тобто способи (методи) використання виділених коштів і ресурсів.

- Сумісність. Мається на увазі те, що концепція перетворення якого-небудь об’єкту повинна гармонійно вписуватися в систему перетворень взаємопов’язаних в єдину систему об’єктів, одним з компонентів якої він є.

- Відкритість. Розроблена концепція повинна давати можливість в її рамках реагувати на зміну умов реалізації концепції і вносити корективи в реалізацію в разі їх необхідності.

Вищевказані вимоги диктують в якості обов'язкової умови включення в логічну структуру концепції наступних позицій:

- виявлення об'єкта і предмета, визначення їх сутності, місця серед множини інших;
- чітке формулювання ролі реалізації концепції і завдань, що стоять при її реалізації;
- виділення умов, необхідних і достатніх для реалізації концепції, і зіставлення їх з реально існуючими;
- визначення кола заходів, що забезпечують перетворення об'єкта реалізації концепції, а також шляхів її реалізації;
- формулювання критеріїв успішності заходів щодо розробки концепції, а також з оцінки результатів її реалізації.

Концепція безпеки підприємства являє собою офіційно затверджений документ, в якому відображена система поглядів, вимог і умов організації заходів безпеки персоналу і власності підприємства. Орієнтовна структура концепції може виглядати наступним чином:

Опис проблемної ситуації у сфері безпеки підприємства:

- перелік потенційних і реальних загроз безпеці, їх класифікація і ранжування;
- причини та фактори зародження загроз;
- негативні наслідки загроз для підприємства.

Механізм забезпечення безпеки:

- визначення об'єкта і предмета безпеки підприємства;
- формулювання політики і стратегії безпеки;

- принципи забезпечення безпеки;
- мета забезпечення безпеки;
- завдання забезпечення безпеки;
- критерії та показники безпеки підприємства;
- створення організаційної структури з управління системою безпеки підприємства.

Заходи з реалізації заходів безпеки:

- формування підсистем загальної системи безпеки підприємства;
- визначення суб’єктів безпеки підприємства та їх ролі;
- розрахунок коштів та визначення методів забезпечення безпеки;
- контроль і оцінка процесу реалізації концепції.

Необхідно мати на увазі, що найбільш повне уявлення про систему безпеки підприємства можна отримати після вивчення офіційно прийнятих документів по концепції безпеки підприємства, комплексної програми забезпечення безпеки підприємства та планів підрозділів підприємства з реалізації цієї програми. Сформована на науковій основі система безпеки підприємства є організаційною основою створення її структурного підрозділу – служби безпеки [14].

3.3 Аналіз аномалій мережевого трафіку інформаційно-обчислювальних систем

Розвиток обчислювальних засобів та інформаційних технологій призводить до автоматизації різних процесів практично у всіх сферах життя суспільства: збільшуються обчислювальні потужності комп'ютерних засобів, удосконалюються технології мережевої взаємодії, змінюються формати і вимоги до побудови інформаційних систем. Через такий розвиток мережеві оператори

вимушені здійснювати моніторинг властивостей трафіку щоб підвищити віддачу від інвестицій, підтримувати рівень сервісу і захистити мережеві ресурси.

На основі аналізу та обробки даних, які отримуються від спеціальних модулів контролю трафіку, необхідно формувати цілісну картину роботи мережі у вигляді логічної схеми стану контрольованих об’єктів. Для цього заздалегідь оброблену інформацію необхідно передавати для зберігання й подальшої обробки на спеціалізовані сервери – CDR (сервери детальної реєстрації викликів) і сервери Frod-менеджменту – FMS. При цьому доступ до спеціалізованих додатків системи повинен забезпечуватися через робочі місця операторів дружніми інтерфейсами.

Завдання аналізу трафіку з метою виявлення та врахування його аномалій полягає в знаходженні компромісу між інтервалом спостереження і детальністю опису. Такий підхід можливий тільки при детальному вивченні природи трафіку і топології мережі. У ідеалі і, отже, кінцевою метою рішення задачі, може бути синтез методу перетворення топології мережі з урахуванням ефектів агрегації для забезпечення можливості проведення експериментів перевірці валідності всіляких теоретичних методів оцінки магістрального трафіку.

Технології моніторингу і виявлення аномалій розділяються за джерелами і типами даних, механізмами виявлення і часу реагування. Аномалії в поведінці трафіку визначають характер збоїв в мережі, якими можуть бути, наприклад, необґрунтоване зростання або падіння інтенсивності трафіку, зміни в стаціонарному характері трафіку, надмірне підвищення інтенсивності використання окремих частин мережі і т.д. Як правило, це свідчить або про ненадійну роботу апаратурної частини, або про зовнішні втручання (зокрема – атаки на мережеві ресурси, що ведуть до різкого необґрунтованого збільшення трафіку) [14].

Виявлення і розпізнавання аномальної поведінки мережі адміністраторами часто ґрунтується на методах, відомих як «ad hoc», тобто на методах спеціальних, суб’єктивних, таких, що з’явилися в процесі довготривалої роботи у області

управління мережею. Аномалії у зв’язку зі збоєм апаратно-програмного забезпечення вельми характерні в умовах, коли матеріальна база створюється в обмежених фінансових можливостях. Дана ситуація типова для сучасного ринку телекомунікаційних послуг, які надаються сучасним підприємствам в Україні. На рис. 3.1. відображений приклад таких аномалій для спостережуваного трафіку з п’ятихвилинним усереднюванням.

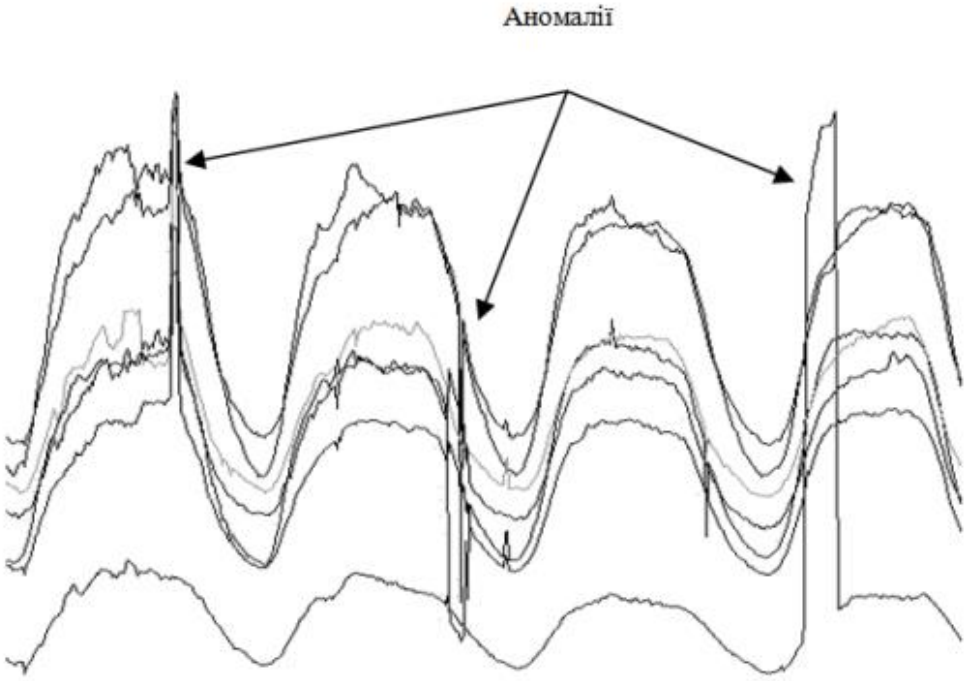

Рис. 3.1. Аномалії трафіку

Слешдот-аномалія (Slashdot або Flash crowds) – аномалія, яка, по суті, є могутнім сплеском відвідуваної ресурсу мережі, після того, наприклад, як посилання на цей ресурс з’являлося на стрічці новин популярного мережевого видання або блога. Термін і саме явище з’явилися завдяки популярному інформаційному технологічному блогу Slashdot. Саме тоді була вперше відмічена дана аномалія, яка на сьогоднішній день часто виявляється. Для даного ефекту є характерним те, що гігантське збільшення трафіку наростає стрімко, фактично перетворюючись на DDoS-атаку, так що сайт, який не розрахований на таку кількість відвідувачів, дуже швидко стає недоступним або доступ до нього стає надзвичайно важким через перевантаженість сервера або недостатньої пропускної

спроможності каналів зв’язку (рис. 3.2.). Слешдот-ефект володіє такою руйнівною силою через часовий чинник, тобто через різкі зміни стану мережі в короткий часовий дискрет.

Рис. 3.2. След-шот аномалія

Як показали практичні спостереження, проведені впродовж останнього року, найчастіше аномалії виникають в результаті різних атак. Наприклад, встановлено, що так звана DoS/DDoS-атака переслідує своєю метою вивести об’єкт з робочого стану. Звичайно, в більшості випадків глобальна атака приводить до великих фінансових втрат того суб’єкта, який атакується. Наприклад, якщо який-небудь комерційний сайт стає недоступним на декілька годин, то це завдасть шкоди бізнесу, а якщо на тиждень, то наслідки можуть бути ще більш катастрофічними.

Аналогічна ситуація характерна і для локальних мереж. Річ у тому, що одним з ефектів популярних атак DoS (Denial of Service), є величезний трафік, що направляється на жертву. Якщо для великої фірми це не такий важливий інцидент, якому варто приділяти першорядну увагу, то для невеликого підприємства навіть середня атака може загрожувати розоренням. Окрім величезної шкоди, що наноситься жертві, такі напади відрізняються простотою і величезною ефективністю. Проти них немає стовідсоткового захисту. Атаки TCP

SYN Flood і TCP-flood, які відносяться до того ж класу блокування роботи мережі, переслідують метою перевищити обмеження на кількість з'єднань, які знаходяться в стані установки. Як показав аналіз, вони організовуються на базі комп'ютерних вірусів. На рис. 3.3 відображений приклад аномального трафіку в результаті TCP-flood-атаки, проведеної на базі впровадження вірусу.

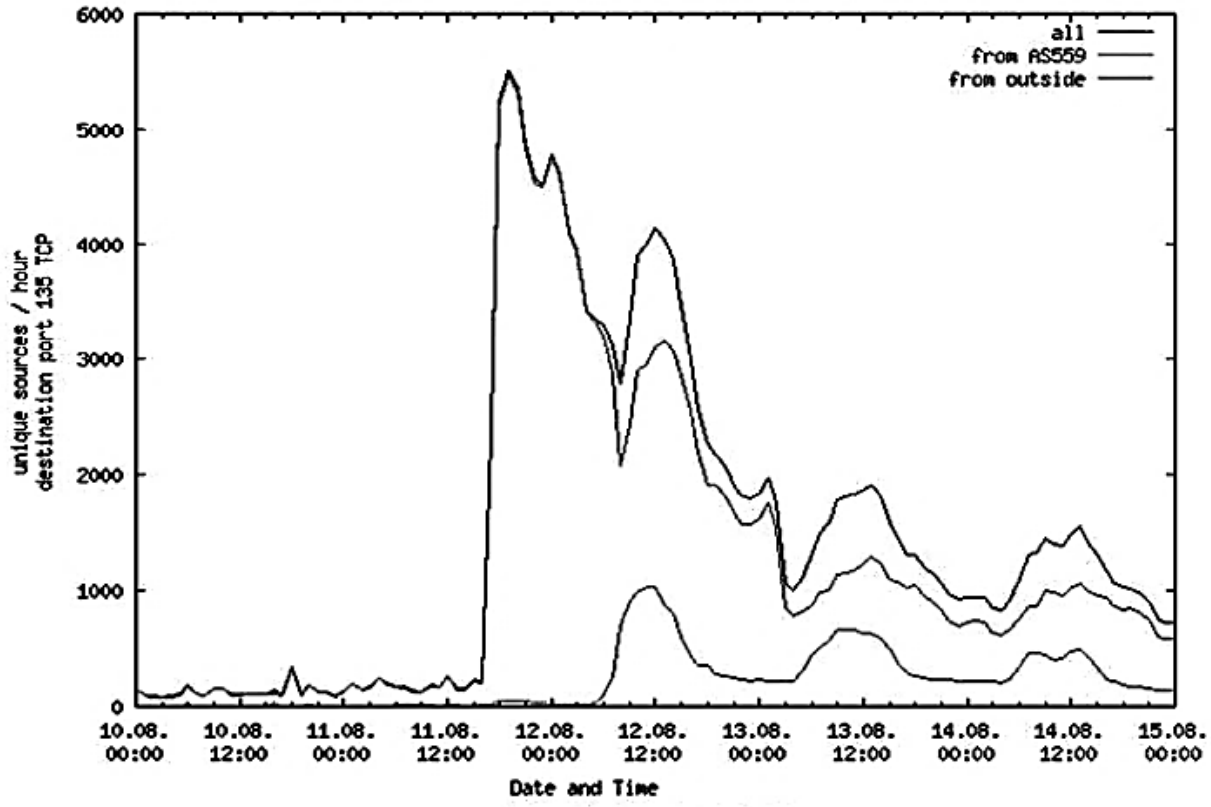

Рис. 3.3. Аномальний трафік під час TCP-flood-атаки

Практичні роботи показали, що аномальний трафік спостерігається при виникненні ситуації нестабільності маршрутів, коли маршрутизатор з високою частотою анонсує маршрут в певну мережу через різні маршрутизатори призначення чи ж чергує анонси відповідними анонсами про недоступність даної мережі.

Близька ситуація – нестабільність мережевого інтерфейсу. Наприклад, унаслідок апаратного збою пристрій попеременно визначає стан свого мережевого інтерфейсу як «робочий», «не робочий». До нестабільності маршруту приводять аварії в мережі, викликані апаратними або програмними збоями, випадковими

помилками на лініях зв'язку, ненадійними з'єднаннями і т.д., що в свою чергу призводить до того, що частина маршрутної інформації пропадає і з'являється знову (рис. 3.4).

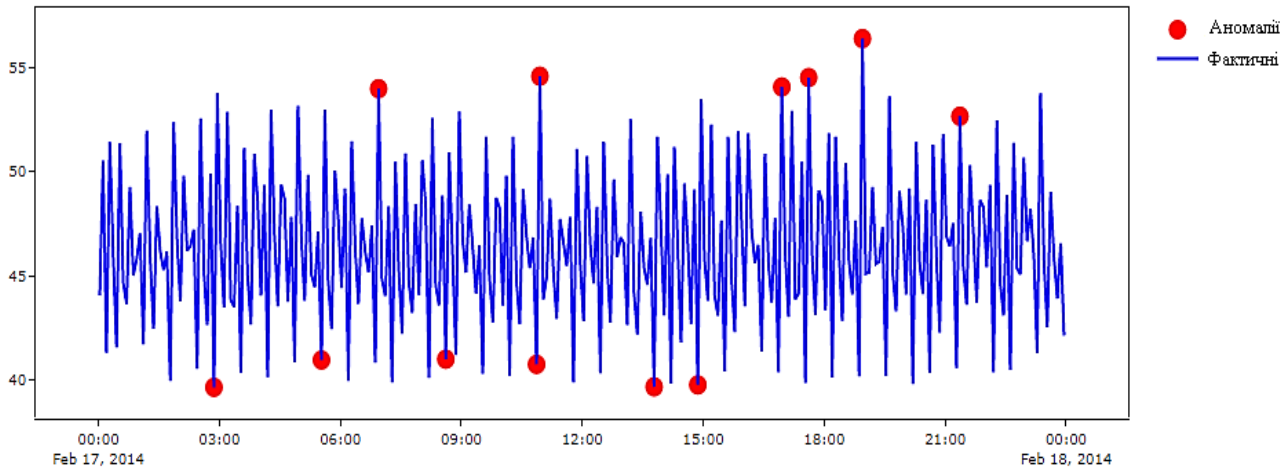

Рис. 3.4. Аномалії в трафіку

У мережах, де для побудови таблиць маршрутизації використовується протокол, в основі якого лежить протокол маршрутизації стану каналу (linkstate), нестабільність маршрутів приводить до частого перерахунку топології всім маршрутизаторам в одному домені маршрутизації. У мережах з дистанційно-векторними (distance vector) протоколами маршрутизації, нестабільність маршрутів спричиняє за собою часту розсилку повідомлень про зміну маршрутів. У обох випадках це перешкоджає збіжності мережі, тобто стану, в якому всі маршрутизатори використовують однакове розуміння поточної мережевої топології. Після порушення збіжності потрібен час для того, щоб маршрутизатори обмінялися інформацією для відновлення збіжності нової мережевої топології [14].

Відзначається, що для умов економіки, що розвивається, можлива наявність аномального трафіку через різні зовнішні причини: силове обмеження потоків, внесення пріоритетності, дія різних політичних подій, указів і т.д. Часто ці аномалії вимагають детальнішої інформації для пояснення. Приклад їх приведений на рис. 3.5.

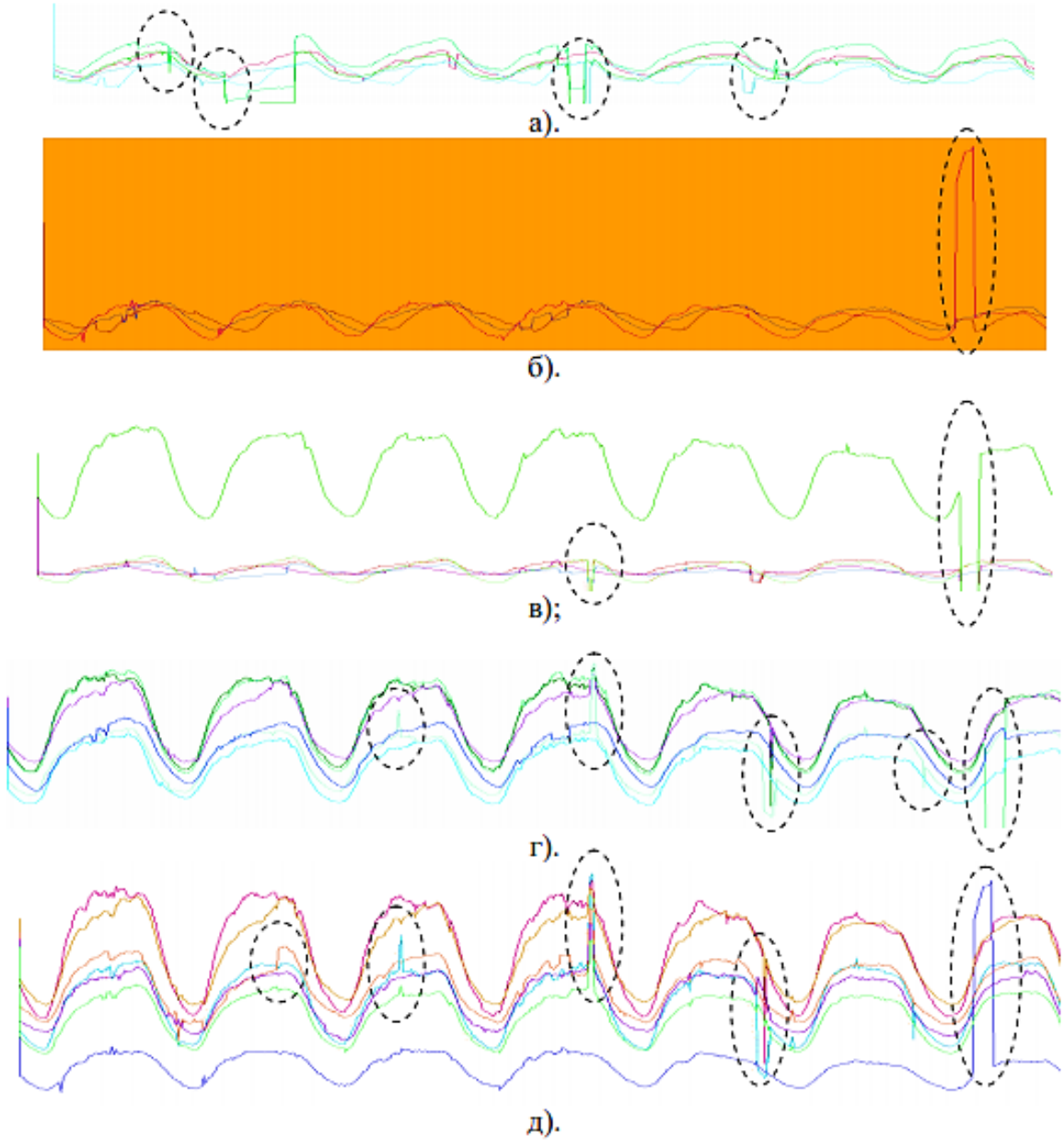

Рис. 3.5. Аномалії трафіку що вимагають уваги

Важливим моментом при розробці моделей дослідження або моделювання трафіку, є отримання інформації щодо використання Wi-Fi-технологій в комплексних системах телекомунікацій, які використовуються фінансовими підприємствами [22].

На сьогодні, в умовах економічної кризи, Wi-Fi по праву може вважатися однією з найбільш перспективних технологій в Інтернет-індустрії, зручній у використанні і оптимальній по співвідношенню «ціна-якість». Стандарт Wi-Fi

дозволяє фінансовим установам надавати високошвидкісний доступ до всіх ресурсів мережі Інтернет, як своїм корпоративним клієнтам, так і власникам ноутбуків і кишенькових комп’ютерів. У зоні покриття мережі Wi-Fi можливо підключення будь-якого пристрою, оснащеного відповідним модулем, що підтримує стандарт IEEE 802.11. Технологія забезпечує одночасну роботу в мережі декількох десятків активних користувачів. Швидкість передачі інформації для кінцевого абонента може досягати 54 Мбіт/с. Пропускна спроможність стандарту може бути порівняна з пропускною спроможністю високошвидкісної виділеної лінії. У містах з історичними пам’ятниками, де прокладка кабелів особливо скрутна, перевага такого підходячи очевидно. Але, як показали спостереження, мінуси все ж таки є. Так, число випадкових чинників при використанні радіоканалу істотно зростає, що спричиняє за собою ще більш стохастичний характер трафіку (рис. 3.6).

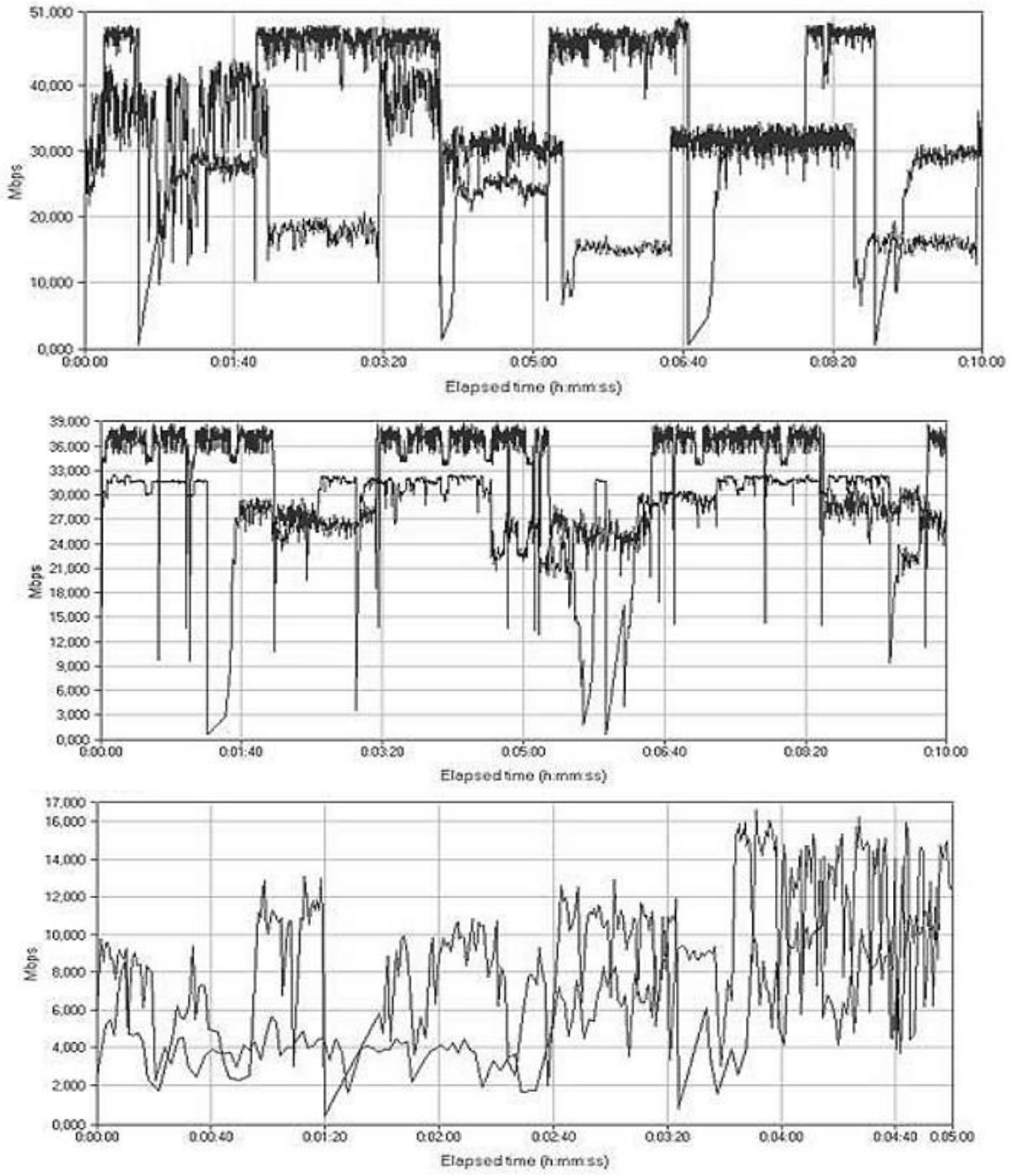

Рис. 3.6. Стохастичний характер трафіку

Характерно, що в мережевому трафіку Wi-Fi спостерігаються періодичні провали як при передачі даних від маршрутизатора до бездротового адаптера, так і у зворотному напрямі. Швидкість передачі даних між двома бездротовими адаптерами може впасти по безлічі причин. Іноді виникають ситуації, коли неможливо встановити з’єднання. Отже, дослідження статистичних закономірностей трафіку Wi-Fi-мереж, є перспективною проблемою подальших досліджень стосовно питань аналізу трафіку.

Як видно з наведених матеріалів, в результаті аналізу окремих аномалій мережевого трафіку в магістральних каналах зв’язку показано, що обробка статистичних даних мережевого трафіку може бути основою для організації їх експорту з загального масиву для зовнішніх додатків і проводити облік аномалій для підвищення якості сервісу, що надається, і організації захисту даних. При аналізі виявлені аномалії мережевого трафіку, облік яких необхідний при моделюванні роботи всіляких мережевих додатків [14].

Висновки до третього розділу

Отож роблячи висновки до розділу можна визначити, що в загальному вигляді технічна документація це досить важливий аспект системи безпеки який врегулює функції захисту інформації, закріпить основоположні принципи побудови системи безпеки, забезпечить детальний опис процедур роботи з інформацією та порядок дій в надзвичайних ситуаціях.

Також не малу роль відіграє побудова концепції безпеки яка дозволить врегулювати та направити сили для побудови надійної системи. А для підтримки системи безпеки в належному стані, мережеві оператори вимушені здійснювати моніторинг властивостей трафіку щоб підвищити віддачу від інвестицій, підтримувати рівень сервісу і захистити мережеві ресурси.

ВИСНОВОК

1. В результаті вивчення сучасного стану технологій стало відомо, що інформаційна безпека є невід'ємною складовою системи безпеки будь якого підприємства. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку. Тож в роботі були розглянуті основні принципи організації інформаційної безпеки на підприємстві які дозволили детально вивчити як саме спланувати організувати та використовувати систему безпеки підприємства для впевненого його розвитку.

2. Було розглянуто методи тестування та аналізу інформаційної безпеки на прикладі експоненціальних моделей Шумана, Джелінскі-Моранді та структурної моделі Нельсона, які дозволять оцінити надійність та розрахувати число відмов програмного забезпечення. Наведений приклад використання даних моделей дозволяє порівнювати різні засоби тестування та обрати серед них най біль раціональний, з точки зору їх можливостей та необхідного рівня аналізу інформаційної системи.

3. Обробка результатів даної роботи показала, що для організації та управління інформаційною безпекою підприємства потрібен цілий комплекс принципів та засобів для надійного функціонування інформаційної системи, що дозволять управляти та корегувати правильне використання інформаційних ресурсів з деякою впевненістю, що вони під надійним захистом.

4. Таким чином мета роботи досягнута: було розглянуто особливості організації інформаційної безпеки підприємства.

Практична значимість дипломної роботи полягає в тому, що її матеріали та результати можуть бути використані при проектуванні надійної системи безпеки підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арапова А. Система управління ризиками як необхідна складова забезпечення кібербезпеки. URL:http://repository.mdu.in.ua/jspui/bitstream/123456789/658/1/kiberbezpeka_2018.pdf
2. Архипов О. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Архипов, А. Скиба // Захист інформації. – 2013. – Т. 15, № 4. – С. 366–375.
3. Богуш В. М., Кривуца В. Г., Кудін А. М., Інформаційна безпека: Термінологічний навчальний довідник/ За ред. Кривуци В. Г. К., 2004. 508 с.
4. Вадим Гребенніков, Модель порушника безпеки інформації в ІТС / Комплексні системи захисту інформації. Проектування, впровадження, супровід // URL: https://it.wikireading.ru/1000009747
5. Василенко М. Підвищення стану кібербезпеки інформаційно комунікаційних систем: якість у контексті вдосконалення інформаційного законодавства / М. Василенко // Юридичний вісник. – № 3. – 2018. – С. 17–24.
6. Верескун М. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М. Верескун // Економіка і організація управління. – 2014. – Вип. 1–2. – С. 54–60.
7. Войнаренко П., Рзаєв Г., Рзаєва Т. Інформаційна безпека підприємства у динамічному ринковому середовищі. URL:http://elar.khnu.km.ua/jspui/bitstream/123456789/1889/1/VOYNARENKO.pdf.
8. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кібер-ризиків. URL: http://zt.knteu.kiev.ua/files/2018/03(98)/10.pdf.
9. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О. В. Герасименко, А. В. Козак. – 2015. – №2.
10. Довгань О. Корпоративна культура кібербезпеки суб’єктів наукової та

науково-технічної діяльності / О. Довгань, А. Тарасюк // Інформація і право. – № 2 (25). – 2018. – С. 51–61.

11. Доктрина інформаційної безпеки України: Затверджена указом Президента України від 25 лютого 2017 року №47/2017. Київ: Офіційний вісник України, 2017. № 20. (4)
12. Завгородня М. Можливості та ризики використання цифрових технологій у промисловості.URL:https://ir.kneu.edu.ua/bitstream/handle/2018/31551/ZE_2019_55.pdf?sequence=1&is Allowed=y.
13. Збожинський С. Інформаційна безпека під час застосування цифрових технологій. URL: http://yur–gazeta.com/publications/practice/zahist–intelektualnoyi–vlasnosti–avtorske–pravo/informaciyna–bezpeka–pid–chas–zastosuvannya–cifrovih–tehnologiy.html.
14. Звіт про науково-дослідну роботу / Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів / О.О. Скопа, Н.Ф. Казакова, О.В. Орлик
15. Іванова В. Інформаційна безпека як підсистема в системі економічної безпеки підприємства. URL: http://eprints.kname.edu.ua/38599/1/67–71.pdf.
16. Інформаційна безпека підприємства у динамічному ринковому середовищ М.П. Войнаренко, Г.І. Рзаєв, Т.Г. Рзаєва / Хмельницький національний університет 2014р.
17. Інформаційна загроза. URL: https://uk.wikipedia.org/wiki/Інформаційна_загроза
18. Казакова Н., Вавілов Є. Автоматизація процесу адаптації інформаційних систем до інцидентів інформаційної безпеки. URL:http://dspace.oneu.edu.ua/jspui/bitstream/123456789/1501/1/Автоматизація%20процесу%20адаптації%20інформаційних%20систем%20до%20інцидентів%20інформаційної%20безпеки.pdf
19. Кириленко А., Бабинюк О. Кібербезпека на захисті бізнесу. URL: https://ir.kneu.edu.ua/bitstream/handle/2018/31417/ZE_2019_118.pdf?sequence=1.

20. Кримінальний кодекс України: Затверджений указом Президента України від 5 квітня 2001 року № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
21. Лисенко Ю. Модель ефективності ІТ-аутсорсингу в контексті розвитку інформаційних систем економічних об'єктів / Ю. Лисенко, Є. Бізянов // Проблеми економіки. – 2013. – № 2. – С. 190–195.
22. Маракова И.И., Скопа А.А., Сыропятов А.А. Комплексная защита информации в беспроводных системах связи // Матер. IV наук.- конф. Департамента спец. телеком. систем та захисту інформ. та Служби безпеки «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні». – К. : НДЦ «Тезис» НТУУ «КПІ». – 2007. – С.73-75.
23. Новікова А. Питання кібербезпеки у світі юриспруденції. URL: https://sud.ua/ru/news/publication/138379–pitannya–kiberbezpeki–u–sviti–yurisprudentsiyi.
24. Основні складові інформаційної безпеки / URL: https://studfile.net/preview/14517462/page:2/
25. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. URL: http://ibo.tneu.edu.ua/index.php/ibo/article/view/124/123.
26. Печенюк А. / Особливості організації інформаційної безпеки сучасного підприємства /А. Печенюк Подільський державний аграрно-технічний університет м. Кам'янець-Подільський
27. Політологія URL:.https://pidruchniki. com/15341220/politologiya/ponyattya_ vidi_zagroz_natsionalnim_interesam_ natsionalniy_bezpetsi_informatsiyniy_sferi
28. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/
29. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV URL:https://zakon.rada. gov.ua/laws/show/964-15
30. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Офіційний вісник України. 2017. № 91. Ст. 2765.

31. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки Закон України від 9 січня 2007 року № 537-V URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text
32. Рудий Т. Засади захисту інформації в інформаційних системах підприємств / Т. Рудий, Л. Томаневич, О. Руда // Актуальні проблеми економіки. – № 2 (152). – 2014. – С. 551–557.
33. Савельєва Т., Панаско О., Пригодюк О. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства / Т. Савельєва, О. Панаско, О. Пригодюк // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2018. – Т. 1, № 4. – С. 81–89.
34. Сакович Л.М / Порівняльний аналіз моделей надійності програмного забезпечення засобів спеціального зв'язку// Сакович Л.М., Павлов В.П., Лівенцев С.П., Небесна Я.Е. ///Information Technology and Security" № 2(2)-2012
35. Северина С. Інформаційна безпека та методи захисту інформації / С. Северина // Вісник Запорізького національного університету. Економічні науки. – 2016. – № 1. – С. 155–161.
36. Сотниченко В. Інформаційна безпека як базова складова економічної безпеки телекомунікаційного підприємства. URL: http://www.dut.edu.ua/uploads/p_1010_25433567.pdf.
37. Стратегія національної безпеки України: введена у дію Указом Президента від 26.05.2015 р. № 287/2015. Офіційний вісник України, 2015. № 43, Ст. 1353.
38. Шарина М., Володін В. Інформаційна складова економічної безпеки підприємства. URL: http://www.economy.nayka.com.ua/?op=1&z=5176.
39. Шемчук Віктор Вікторович/ Навчально-наукового гуманітарного інституту Таврійського національного університету імені В. І. Вернадського / загрози інформаційній безпеці: проблеми визначення та подолання/ URL: http://maup.com.ua/assets/files/expert/7/23.pdf
40. Экспоненциальная модель Шумана URL:

https://studwood.ru/1627209/informatika/eksponentsialnaya_model_shumana

41. Я.М. Чабанюк / Побудова і дослідження моделі надійності програмного забезпечення з індексом величини проекту / Національний університет "Львівська політехніка" / Я.М. Чабанюк, В.С. Яковина, Д.В. Федасюк, М.М. Сенів, У.Т. Хімка// 2010 р.