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:

ОРГАНІЗАЦІЯ УПРАВЛІННЯ ІНЦИДЕНТАМИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

СТУДЕНТ: Осинський Олександр Олексійович _____
(підпис)

КЕРІВНИК: доцент Якименко Юрій Михайлович _____
(підпис)

НОРМОКОНТРОЛЕР к.т.н., с.н.с. Щебланін Юрій Миколайович _____
(підпис)

Київ – 2020

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Освітньо-кваліфікаційних рівень – Магістр
Галузь знань - «12 Інформаційні технології»
Спеціальність - «125 Кібербезпека»
Спеціалізація - «Управління інформаційною безпекою»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____ 2019 р.

ЗАВДАННЯ

на дипломну роботу

студенту Осинському Олександру Олексійовичу

1. **Тема роботи** «Організація управління інцидентами в системі забезпечення інформаційної безпеки підприємства», затверджена наказом по університету від “14” листопада 2019 р. № 518.
2. **Термін здачі** студентом закінченої дипломної роботи “28” грудня 2019 р.
3. **Вихідні дані до роботи**: проаналізувати вимоги до забезпечення інформаційної безпеки підприємства та на основі аналізу організації управління інцидентами в її системі забезпечення інформаційної безпеки провести дослідження і розробити рекомендації щодо вдосконалення процесів організації управління інцидентами на підприємстві.
4. **Склад розрахунково-пояснювальної записки** (перелік питань до розробки)
1. Аналіз вимог до забезпечення інформаційної безпеки підприємства.
2. Аналіз організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.
3. Дослідження процесів організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.
5. **Перелік обов’язкових демонстраційних креслень**:
1. Схема вимог до забезпечення інформаційної безпеки підприємства.
2. Схема організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.
3. Рекомендації по вдосконаленню процесів організації управління інцидентами на підприємстві (для вибраного прикладу).
4. Презентація доповіді, виконана в Microsoft PowerPoint.
6. **Термін виконання дипломної роботи:**
подання закінченої роботи керівнику 24 грудня 2019 року.
подання роботи на рецензію 28 грудня 2019 року.
7. **Дата видачі завдання** 15.11.2019 року

Керівник: _____ Якименко Юрій Михайлович
(підпис)

Завдання прийняв для виконання _____ Осинський Олександр Олексійович
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «15» _листопада_ 2019 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Відмітка про виконання
1.	Підбір науково-технічної літератури.	18.11.2019	
2.	Аналіз та систематизація матеріалу. вступ	22.11.2019	
3.	Аналіз вимог до управління інцидентами в системі забезпечення інформаційної безпеки організації	29.11.2019	
4.	Дослідження досвіду управління інцидентами в системі забезпечення інформаційної безпеки організації	6.12.2019	
5.	Рекомендації по вдосконаленню процесу управління інцидентами в системі управління безпекою організації(для вибраного прикладу).	13.12.2019	
6.	Підготовка демонстраційного матеріалу	20.12.2019	
7.	Оформлення та друк пояснювальної записки	28.12.2019	
8.	Оформлення презентацій	3.01.2020	
9.	Отримання відгука та рецензії на роботу, та попередній захист на кафедрі	9.01.2020	
10	Захист в ДЕК	14.01.2020	

РЕФЕРАТ

Робота містить вступ, три розділи з підрозділами, висновки та список використаних джерел. Загальний обсяг роботи - 93 сторінок.

Об'єкт дослідження: організація управління інцидентами в системі забезпечення інформаційної безпеки підприємства.

Предмет дослідження: система забезпечення інформаційної безпеки підприємства.

Метою роботи є формулювання основних вимог щодо управління інцидентами в системі забезпечення інформаційної безпеки і розробка рекомендацій щодо вдосконалення її процесів для вибраного прикладу інформаційно-комунікаційної системи організації.

Для досягнення поставленої в роботі мети необхідно вирішити наступні задачі:

- проаналізувати вимоги до забезпечення інформаційної безпеки підприємства.
- провести аналіз організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.
- дослідити процеси організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.

Новизна роботи полягає у тому, що удосконалено алгоритм обробки інцидентів. Практична цінність отриманих результатів полягає у тому, що запропоновано більш надійний та якісний спосіб роботи з інцидентами.

Ключові слова: ІНЦИДЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПРОЦЕС РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах бурхливого розвитку інформаційних технологій та появи наростаючого числа інформаційних загроз основною цінністю для підприємства поступово стають інформаційні ресурси та інфраструктура для їх створення, обробки, передачі, а забезпечення інформаційної безпеки набуває першочергового значення для успішної діяльності бізнесу. В даний час ефективність функціонування бізнесу безпосередньо залежить від інформаційно-комунікаційних технологій.

У процесі вирішення підприємством операційних завдань, обсяг виробленої і споживаної інформації постійно зростає, роблячи значний вплив на позицію компанії на ринку. При постійному зростанні гнучкості бізнес процесів потрібно створювати і впроваджувати сучасні нові ефективні методики, а також впроваджувати кращі практики управління службою підтримки.

Основною частиною системи управління інформаційною безпекою є система управління інцидентами. Дані, що збираються в рамках процесів управління інцидентами інформаційної безпеки, є важливими для роботи значної кількості інших процесів управління інформаційною безпекою, наприклад, для управління доступом, змінами, безперервністю бізнесу, оцінки ефективності вже існуючих захисних заходів. Інакше кажучи, процес управління інцидентами інформаційної безпеки є своєрідним «двигуном» життєвого циклу системи управління інформаційною безпекою.

Розробка процесу управління інцидентами інформаційної безпеки відповідно до кращих практик передбачає наступне:

- визначення ролей і відповідальності всіх співробітників за своєчасне і якісне реагування на інциденти інформаційної безпеки;
- надання інформації для відстеження ефективності прийнятих захисних заходів;
- надання інформації для коректного проведення аналізу ризиків інформаційної безпеки;
- запобігання інцидентів інформаційної безпеки в майбутньому за рахунок оперативного надання відомостей про існуючі інциденти інформаційної безпеки, швидкості реагування на них, аналізу динаміки інцидентів інформаційної безпеки.

Таким чином, можна зробити висновок, що впровадження процесу управління інцидентами допомагає вирішенню проблем, які є у будь-який динамічно розвивається: підвищення збитку від інцидентів інформаційної безпеки, а також принятя рішень, які мінімізують наслідки від можливих загроз інформаційної безпеки.

Виникнення будь-якого інциденту інформаційної безпеки і слабке функціонування системи управління інцидентами можуть чинити негативний вплив на безперервність важливих функцій бізнесу підприємства і підтримують його елементів. В такому випадку необхідним є планування безперервності бізнесу, що є гарантією відновлення штатного функціонування організації в разі будь-якого інциденту, в тому числі і інциденти інформаційної безпеки. Процес забезпечення

безперервності бізнесу також дає впевненість в тому, що відновлення всіх важливих функцій бізнесу в робочий стан досягається за урахуванням заданих пріоритетів і за рахунок застосування потрібних планових засобів і заходів.

Тому перед будь-яким підприємством рано чи пізно постають наступні питання:

- наскільки для неї критичний певний ризик переривання бізнесу;
- як уникнути такого ризику або максимально мінімізувати негативні наслідки;
- що потрібно зробити заздалегідь;
- як знайти баланс між допустимими інвестиціями в превентивних заходів (по мінімізації переривань їх наслідків) і можливими втратами.

Існуючі стандарти і підходи при вирішенні завдань, що стосуються управління якістю процесів, безпосередньо впливають на бізнес мають деякі недоліки. Наприклад, в області управління IT-послугами по суті не існує відповіді на питання за допомогою яких методів і підходів потрібно управляти якістю процесів. Таким чином тема розробки методики управління якістю процесів дозволу інцидентів є актуально. Глибоке вивчення даної теми дозволить значно підвищити якість управління інцидентами при реалізації IT-послуг.

Метою роботи є формулювання основних вимог щодо управління інцидентами в системі забезпечення інформаційної безпеки і розробка рекомендацій щодо вдосконалення її процесів для вибраного прикладу інформаційно-комунікаційної системи організації. Для досягнення поставленої в роботі мети необхідно вирішити наступні задачі:

- проаналізувати вимоги до забезпечення інформаційної безпеки підприємства.
- провести аналіз організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.
-дослідити процеси організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.

У першому розділі основного тексту розглядаються вимоги щодо забезпеченяя інформаційної безпеки підприємтсва, а саме основні характеристики інформаційної безпеки підприємства, та вимоги стандартів з управління інцидентами інформаційної безпеки.

У другому розділі досліджується саме впровадження системи забезпечення інформаційної безпеки, методичні подходи до організації управління інцидентами в системі забезпечення інформаційної безпеки та досвід організації управління інцидентами.

У третьому розділі - на основі результатів, отриманих у першому і другому розділах, розроблені рекомендації щодо вдосконалення організації процесів управління інцидентами повязанами із роботою пресоналу та їх розслідування та інциденти у кібернетичному просторі, метрики інцидентів інформаційної безпеки, для вибраного прикладу та основні рекомендації.

1 АНАЛІЗ ВИМОГ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМТСВА

1.1 Основні характеристики інформаційної безпеки підприємства

У сучасних умовах перед підприємствами та організаціями гостро постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, що становлять комерційну або державну таємницю.

Успіх виробничої і підприємницької діяльності в чи малому ступені залежить від уміння розпоряджатися таким найціннішим товаром, як інформація, але вигідно використовувати можна лише ту інформацію, яка потрібна ринку, але невідома йому. Тому в умовах посилення конкуренції успіх підприємництва, гарантія отримання прибутку все більшою мірою залежать від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал і конкретну технологію.

Підприємницька діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Однак захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємця. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями (властивостями), як корисність, своєчасність і достовірність відомостей які надходять.

Інформаційна безпека - це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення. Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають [1].

Основними цілями інформаційної безпеки підприємства є:

• конфіденційність інформації, тобто необхідність введення обмежень доступу до даної інформації для певного кола осіб;

• неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб;

• цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка і виведення), яка полягає в її існуванні в неспотвореному вигляді (незміненому по відношенню до деякому фіксованому її станом);

• доступність інформації, тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до цікавлячої їх інформації;

• мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів;

• облік усіх процесів, пов'язаних з ризиками.

Досягнення заданих цілей здійснюється в ході вирішення наступних завдань:

• введення в систему термінів інформаційної безпеки;

• класифікації інформаційних ресурсів підприємства;

• визначення власників процесів, відповідальних за інформаційну безпеку;

• розробки спектра ризиків інформаційної безпеки та проведення їх експертних оцінок;

• визначення групи доступу до інформаційних ресурсів;

• розробки системи управління ризиками інформаційної безпеки (методи та їх оцінка);

• складання переліків адміністративних і технічних заходів для мінімізації та компенсації ризиків;

• здійснення заходів інформаційної безпеки та періодичного контролю за станом ризиків;

• забезпечення фізичної безпеки та безпеки персоналу;

• розробки вимог до інформаційної системи з погляду інформаційної безпеки;

• контролінгу інформаційної безпеки на підприємстві.

Інформаційна безпека організації - цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Захист інформації - це комплекс заходів, направлених на забезпечення інформаційної безпеки. Таким чином, правильний з методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів

інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС).

Загрози інформаційній безпеці - це зворотна сторона використання інформаційних технологій [1].

В Україні забезпечення ІБ здійснюється шляхом захисту інформації — у випадку, коли необхідність захисту інформації визначена законодавством в галузі ЗІ. Для реалізації захисту інформації створюється комплексна система захисту інформації (КСЗІ). Або створюється система захисту основана на:

• міжнародних стандартах ISO/IEC 27001 та ін. - для підтримки рішень на основі ITIL та COBIT і виконання вимог англ. Sarbanes-Oxley Act (акту Сербайнза-Оклі про відповідальність акціонерів за обізнаність про стан своїх активів). Тоді на підприємстві створюється система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі ІБ.

• власними розробками (тобто інші варіанти, які не включені до міжнародних стандартів та законодавства, але вони є необхідними на думку керівництва).

Оскільки визначення поняття «суб'єкти забезпечення інформаційної безпеки України» нормативно не закріплено в Законі України «Про основи національної безпеки України», Стратегії національної безпеки України та Доктрині інформаційної безпеки України, вважаю за необхідне висловити авторське розуміння поняття «суб'єкти забезпечення інформаційної безпеки України».

Суб'єктами забезпечення інформаційної безпеки України є система державних і недержавних інституцій, а також громадян України об'єднаних спільною метою щодо захисту національних інтересів в інформаційній сфері. Отже, коло суб'єктів забезпечення інформаційної безпеки України представляє собою багаторівневу систему, що має спільну мету - забезпечення інформаційної безпеки України, але різні повноваження, можливості, засоби тощо [1].

Суб’єкти впливу на інформаційну систему підприємства поділяються на 2 групи:

- зовнішні (злочинці, хакери, їх об’єднання тощо);
- внутрішні (персонал, який має доступ до інформаційних систем та технічних засобів підприємства).

Також є суб’єкти які здійснюють заходи з забезпечення ІБ підприємства:

- Керівництво

- Служба ІБ (це самостійний підрозділ підприємства, яке займається вирішенням проблем інформаційної безпеки даної організації. Служба інформаційної безпеки повинна бути самостійним підрозділом і підкорятися безпосередньо першій особі в організації)
- Керівники функціональних підрозділів (це начальники управлінь, начальники підпорядкованих їм служб, відділів, лабораторій, секторів, груп. А ще у кожного начальника є заступник і, часом, не один).

Суб'єкти представляють сутності, між якими поділяються інформаційні ресурси. Це можуть бути легальні користувачі інформаційних систем (ІС): персонал, який підтримує роботу ІС, зовнішні і внутрішні клієнти; групи легальних користувачів, що об'єднані по різним ознаках. Користувач здійснює доступ до об'єктів ІС не безпосередньо, а за допомогою прикладних процесів, які запускаються від його імені.

Варто зазначити, що на стан інформаційних систем можуть вплинути так звані «природні» фактори, тобто фактори, не зумовлені несанкціонованими діями суб'єктів.

Об'єкт можна визначити як середовище, пов'язане із створенням, перетворенням, розповсюдженням і споживанням інформації і яке забезпечує життєдіяльність певної системи.

Об'єкти представляють фізичні і логічні інформаційні ресурси. До фізичних ресурсів належать як окремі пристрої повністю (процесор, зовнішні пристрої, маршрутизатори, комутатори, фізичні канали зв'язку і т. п.), так і фізично поділювані ресурси пристрою (розділи і сектори диску, процесорний час, фізичні з'єднання каналу зв'язку). Логічними ресурсами є файли, обчислювальні процеси, мережеві сервіси, додатки, пропускна спроможність каналів зв'язку і т. п.

Операції виконуються суб'єктами над об'єктами. Для кожного типу об'єктів існує власний набір операцій, які з ними може виконувати суб'єкт. Наприклад, для файлів це операції читання, записи, видалення, виконання; для принтера – друк, перезапуск, очищення черги документів, припинення друку документа; для маршрутизатора – конфігурування і т. д.

Система контролю доступу вирішує, які операції дозволені для даного суб'єкта по відношенню до даного об'єкту. Для автоматизованого контролю доступу необхідно, щоб для кожної пари «суб'єкт-об'єкт» були однозначно визначені правила доступу, на підставі яких система могла б дозволити або

заборонити виконання кожної з передбачених для даного об’єкта операції. Найважливішими елементами керованого доступу є процедури ідентифікації, автентифікації і авторизації [1].

Ідентифікація – це присвоєння об’єктам і суб’єктам інформаційної системи унікальних імен – ідентифікаторів. Лише при наявності унікальних ідентифікаторів система отримує можливість розпізнавати і оперувати суб’єктами і об’єктами. Одні ідентифікатори автоматично генеруються ОС і додатками (ідентифікатори процесів, ідентифікатори логічних мережевих з’єднань), інші призначаються адміністратором комп’ютерної мережі (ідентифікатори користувачів, адреси комп’ютерів, доменні імена мережевих сервісів), треті породжуються звичайними мережевими користувачами, що володіють таким правом (вибір власного імені, призначення імен файлів) [1].

Ідентифікація користувачів є процедурою, що виконується при логічному вході в систему, коли користувач у відповідь на виведене на екрані запрошення вводить свій ідентифікатор (ім’я), а система, звіряючись зі своїми даними, визначає, чи входить дане ім’я в число імен зареєстрованих (легальних) користувачів. Користувач може бути представлений в системі у вигляді декількох суб’єктів і відповідно мати кілька користувацьких ідентифікаторів.

Автентифікація – це процедура підтвердження суб’єктом/об’єктом того, що він є те (тим), за що (кого) він себе видає. Автентифікація, або, іншими словами, процедура встановлення автентичності, може застосовуватися як до користувачів, так і до інших об’єктів і суб’єктів, зокрема до даних, програмами, додатків, пристроїв, документів.

Автентифікація даних означає доказ їхньої автентичності, тобто того, що вони поступили в незміненому вигляді і саме від того суб’єкта, який оголосив про це. У процедурі автентифікації беруть участь дві сторони: автентифікований доводить свою автентичність, пред’являючи деякий доказ – автентифікатор; автентифікуючий перевіряє ці докази і приймає рішення. Автентифікація буває односторонньою і двосторонньою (взаємною).

Авторизація – це процедура контролю доступу суб’єктів (користувачів, обчислювальних процесів, пристроїв) до об’єктів (файлів, додатків, сервісів, пристроїв) і надання кожному із них саме тих прав, які для них визначені правилами доступу. На відміну від автентифікації, яка дозволяє розпізнати легальних і нелегальних користувачів, авторизація стосується лише легальних

користувачів, які успішно пройшли процедуру автентифікації. Доступ до об’єктів, який отриманий в обхід дозволу системи контролю доступу, називається несанкціонованим, або неавторизованим [2].

Вразливість (Vulnerability) – це слабка ланка інформаційної системи, яка, ставши відомою зловмисникові, може дозволити йому порушити її безпеку. Вразливими є, наприклад, помилка в програмі, примітивний пароль, неправильне призначення прав доступу до файлу з важливими даними і безліч інших дефектів в розробці, експлуатації або налаштування системи. Вразливості системи можуть бути прихованими, тобто ще не виявленими, відомими, але тільки теоретично, або ж загальновідомими, які активно використовуються зловмисниками.

Загроза (Threat) – набір обставин і дій, які потенційно можуть призвести до порушення безпеки системи (тобто до порушення її конфіденційності, цілісності і доступності. Загрози бувають технічні, що виходять з штучно створеного людиною світу техніки і технологій (зокрема, з Інтернету), а також загрози, що виникають від природних катаклізмів, військових дій, терористичних атак або економічних потрясінь [3].

Атака (Attack) – це реалізована загроза. Атака може відбутися тільки тоді, коли одночасно існують вразливість і спрямована на використання цієї вразливості загроза.

Збиток (Loss, Impact) – це негативний вплив на систему, який є наслідком успішної атаки.

Схематичний вид зв'язків між цими поняттями представлений на рис. 1.1.

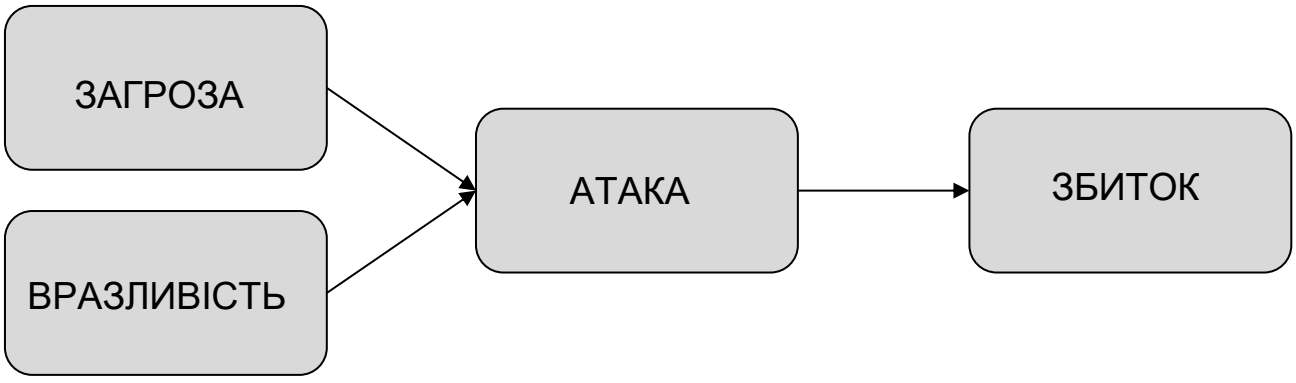

Рис. 1.1. Логічний зв’язок між поняттями «вразливість», «загроза», «атака», «збиток»

Класифікація загроз безпеці інформації на підприємстві. Основним об'єктом впливу загроз безпеки є інформація, що обробляється в автоматизованих системах установи (АС). Базисом АС є: загальносистемне програмне забезпечення (ПЗ), програмні оболонки, програми загального призначення, текстові процесори, редактори та інтегровані пакети програм. Особливе місце в загальносистемному ПЗ займають системи управління базами даних. Інформація в АС може надходити з автоматизованого робочого місця (далі - АРМ) локальної мережі по внутрішнім і по зовнішніх каналах зв'язку, при цьому інформація може вводитися як з клавіатури, так і з зовнішніх носіїв інформації. Крім того, АС може використовувати інформаційні ресурси інших установ і організацій та ресурси глобальних телекомунікаційних мереж. До користувачів АС відносяться всі зареєстровані в ній особи (організації), наділені певними повноваженнями доступу. В рамках своїх повноважень користувач може здійснювати тільки дозволені йому дії з використанням загальносистемного і прикладного ПЗ [3].

Процес обробки інформації в АС здійснюється під контролем адміністраторів системи, а її захисту - адміністраторів безпеки.

Джерела загроз безпеці інформації підприємства можна розділити на три групи: антропогенні, техногенні та стихійні.

У групу антропогенних джерел загроз безпеки інформації входять:

- кримінальні структури, рецидивісти і потенційні злочинці;
- недобросовісні партнери і конкуренти;
- персонал установи (банку, його філій).

З урахуванням аналізу міжнародного досвіду захисту інформації та досвіду проведення аналогічних робіт у вітчизняних організаціях зловмисні дії персоналу, що працює в установі, можна розділити з урахуванням соціальних передумов, характерних для України, на чотири основні категорії:

1) переривання - припинення нормальної обробки інформації, наприклад внаслідок руйнування обчислювальних засобів. Такі дії можуть викликати дуже серйозні наслідки, якщо навіть інформація при цьому не піддається ніяким впливам;

2) крадіжка - читання або копіювання інформації, розкрадання носіїв інформації з метою отримання даних, які можуть бути використані проти інтересів власника (власника) інформації;

3) модифікація інформації - внесення в дані несанкціонованих змін, спрямованих на заподіяння шкоди власнику (власнику) інформації;

4) руйнування даних - необоротне зміна інформації, що приводить до неможливості її використання.

До техногенних джерел загроз відносяться:

• неякісні технічні засоби обробки інформації;

• неякісні програмні засоби обробки інформації;

• засоби зв'язку, охорони, сигналізації;

• інші технічні засоби, що застосовуються в установі;

• глобальні техногенні загрози (небезпечні виробництва, мережі енерго, водопостачання, каналізації, транспорт і т.п.).

До стихійних джерел загроз відносяться пожежі, землетруси, повені, урагани та інші форс-мажорні обставини [3].

Напрями та завдання інформаційної безпеки на підприємстві умовно виділяються три основних напрямки:

- Організаційно-технічний, в рамках якого створюється оболонка навколо об'єкта захисту, тобто інформаційних ресурсів, з певною мірою надійності виключає або суттєво утрудняє проведення маніпуляцій з інформацією в АС проти інтересів користувачів системи;

- Правовий, спрямований на створення імунітету, заснованого на загрозі застосування репресивного інструменту відносно порушників інтересів користувачів системи, і встановлює механізм застосування санкцій відносно правопорушника;

- Економічний, що передбачає механізм усунення матеріального збитку, завданого власнику інформації в результаті несанкціонованих дій з нею з боку правопорушника.

Організаційно-технічний напрям безпеки інформації є найбільш реальним напрямом у захисті інформації підприємства. У цьому напрямку доцільно виділити два основні завдання:

1) забезпечення цілісності самої інформації і процесів її обробки, передачі та зберігання;

2) забезпечення конфіденційності інформації обмеженого доступу.

При аналізі завдань безпеки інформації введені поняття:

- Обчислювальне середовище (ОС) - повне безліч програм і даних, що розташовуються на внутрішніх накопичувачах АС;
- Операційне середовище (ОСр) - сукупність функціонуючих в даний момент часу елементів обчислювального середовища, що знаходяться в оперативній пам'яті АС;
- Зовнішній компонент ОСр - алгоритми управління АС через канали зв'язку;
- Внутрішній компонент ОСр - елементи ОС даної АС.

Основне положення і розроблені моделі дозволяють виділити два основні класи задач безпеки інформації:
- захист елементів обчислювального середовища;
- забезпечення цілісності даних, процедур обробки та конфіденційності інформації;
- контроль елементів операційного середовища;
- зовнішніх компонентів ОСр, цілісності внутрішніх компонентів ЗСр і семантики даних.

Методи захисту елементів ОС практично зводяться до методів захисту даних, а також до методів авторського захисту програм і даних на етапі їх розробки. Основні способи захисту даних представлені на рис. 1.2.

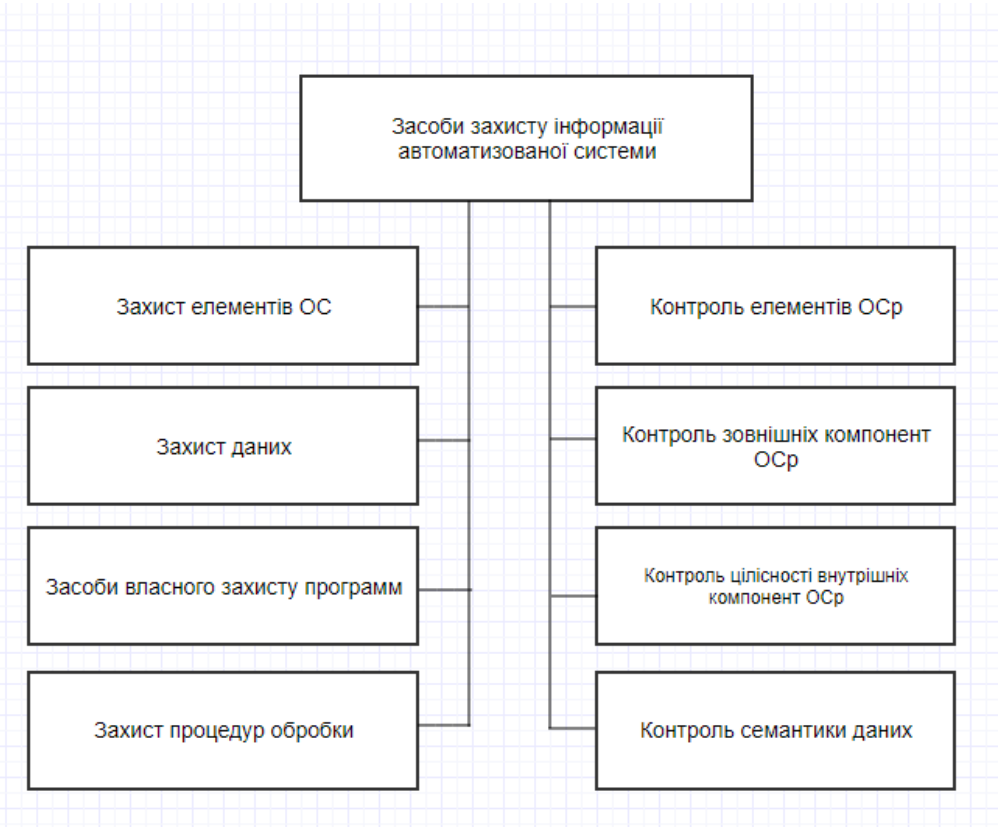

Рис. 1.2. Класифікація засобів захисту інформації в автоматизованій системі.

Системи розмежування доступу (СРД) забезпечують авторизований і санкціонований доступ до окремих груп елементів ОС. До даного класу відносяться різного роду парольні системи та системи ідентифікації користувачів, що обмежують доступ як до системи в цілому, так і до окремих її елементів.

Типова система розмежування доступу включає підсистеми:

• ідентифікації користувача але індивідуальним паролю і заборони роботи з АС незареєстрованим користувачем;

• розмежування доступу до ресурсів для зареєстрованого користувача;

• автоматичної реєстрації дій користувача;

• автоматичного запиту підтвердження особи користувача після закінчення заданої паузи його неактивності;

• контролю за можливими спробами НСД;

• адміністратора безпеки, що здійснює функції ведення списку користувачів і груп користувачів, визначення та зміни повноважень користувачів і т.д.

• контролю цілісності та захисту від копіювання програмного забезпечення.

Методи і способи забезпечення захисту інформації. Захист програм забезпечується:

• захистом авторських прав;

• захистом програм від дослідження і копіювання;

• парольний захистом і захистом від несанкціонованого запуску;

• самотестуванням і самовідновлення виконуваного коду програми.

Питанням захисту авторських прав повинні приділяти увагу насамперед розробники програм.

Для парольного захисту і захисту від запуску програм використовуються ідентифікація користувача і обмеження на кількість запусків або за датою запуску, або з урахуванням кількості запусків.

Для самотестування і самовідновлення виконуваного коду програми вводяться модулі діагностики характеристик виконуваного коду програм: розмір файлу, контрольна сума, перелік контрольних точок і т.п. Крім того, існують алгоритми, здатні відновлювати штатний виконуваний код програми при деяких видах спотворення.

До числа засобів тестування і відновлення відносяться всі відомі антивірусні засоби, так звані полифаги і полідетектори [4].

1.2 Вимоги стандартів з управління інцидентами інформаційної безпеки

Засоби забезпечення захисту інформації на підприємстві. Загальновизнаним є представлення різних засобів захисту у вигляді чотирьох ієрархічно організованих рівнів, засоби кожного з яких можуть бути використані на різних етапах життєвого циклу системи забезпечення інформаційної безпеки. До рівня засобів безпеки відносяться правове регулювання, стандартизація, ліцензування та морально-етичні норми, прийняті в суспільстві. Законодавство може прямо впливати на концепцію побудови захисту. Наприклад, вихід Закону «Про персональні дані», що регламентує заходи щодо забезпечення безпеки персональних даних при їх обробці, вимагає від багатьох підприємств перегляду та внесення принципових змін в процедури і інфраструктуру обробки інформації. Не менш принциповими можуть виявитися вимоги сертифікації засобів захисту даних, які передбачається використовувати в проектованій системі забезпечення безпеки, або необхідність отримання ліцензії для обраного виду діяльності.

Рис. 1.3. Багаторівнева модель засобів захисту від інформаційних загроз.

Інформаційні технології пронизують наше життя, тому цілком природно, що правовідносини в даній сфері вже давно регулюються розвиненим законодавством. Учасниками правовідносин є суб’єкти правовідносин, до яких в області інформаційної безпеки можна віднести власників та споживачів інформації,

власників інтернет-сайтів, провайдерів телекомунікаційних мереж, розробників програмних і апаратних засобів інформаційних технологій та ін.

Права і обов'язки суб'єктів правовідносин визначаються по відношенню до об'єктів правовідносин, до яких належать, наприклад, ІС (державні і приватні), засоби захисту інформації (алгоритми шифрування, апаратні ключі, які використовуються для автентифікації, і т. п.), послуги, що надаються в області ІБ, інформація обмеженого доступу, в тому числі інформація, яка становить державну, комерційну, банківську, сімейну таємницю, таємницю листування, персональні дані та ін.

Необхідність захисту інформаційних ресурсів і підтримуючої їх інфраструктури диктується як нашими правами на захист (наприклад, кожному громадянину має бути забезпечений захист від розкриття його персональних даних), так і обов'язками її захищати (кожна організація, що оперує персональними даними, зобов'язана захищати їх від розкриття) [5].

Нормативно-правовий акт – це офіційний документ, прийнятий компетентним правотворчим органом і встановлює загальнообов'язкове державне розпорядження, розраховане на багаторазове застосування.

Сукупність усіх нормативно-правових актів, що діють на території країни, прийнятих законодавчим (представницьким) органом, називається законодавством. Законодавство включає заходи обмежувально-репресивного характеру, спрямовані на запобігання порушень, в тому числі шляхом застосування 30 покарань (наприклад, кримінальний кодекс), і заходи творчого характеру, спрямовані на координацію робіт у сфері ІБ, навчання і допомогу в створенні і використанні засобів забезпечення інформаційної безпеки (наприклад, стандарти).

До числа порушень законодавства в області ІБ відносять як традиційні «комп'ютерні» злочини, такі як порушення доступності даних (DoS-атаки), використання шкідливого ПЗ, перевищення привілеїв, несанкціонований доступ та ін., так і порушення регламентуючих правил, наприклад відсутність ліцензії на певний вид діяльності в області захисту інформації, використання несертифікованих продуктів там, де це вимагається законом (наприклад, засобів шифрування при роботі з інформацією, що становить державну таємницю).

Засоби безпеки процедурного рівня. Засоби безпеки процедурного рівня вирішують завдання, поставлені адміністративним рівнем, з використанням технічних засобів, що надаються технічним рівнем. В якості основного засобу

процедурного рівня виступає людина, яка виконує взаємопов’язану послідовність дій, спрямовану на вирішення певної задачі забезпечення безпеки.

Будь-який аспект інформаційної безпеки передбачає використання засобів процедурного рівня. Навіть просте підтримання нормального режиму роботи інформаційної системи здійснюється за рахунок виконання безлічі повсякденних процедур: резервного копіювання, управління програмним забезпеченням, профілактичних робіт і т. п. Багато процедур включають в себе застосування технічних засобів. Наприклад, завдання обліку різних ресурсів (документації, програм, обладнання та ін.), як правило, вирішується із залученням спеціально розроблених для цих цілей програм. До засобів процедурного рівня відноситься також фізичний захист: пропускний режим на територію підприємства, охорона кордонів території та ін.

У загальному випадку процедура – це взаємопов’язана послідовність дій, спрямована на вирішення деякої задачі. Процедура може бути формальною, як, наприклад, при її поданні у вигляді алгоритму або програми на мові програмування, так і неформальної, у вигляді певної міри розпливчастих вказівок. Формальні процедури можуть бути реалізовані механічними або електронними пристроями. В умовах неформальних процедур, коли неможливо абсолютно однозначно визначити всі деталі процедури, а саме така більшість процедур безпеки (підтримка працездатності системи, управління персоналом, фізичним захистом, управління документацією і ін.), може діяти лише людина.

Саме тому між рівнями стратегій безпеки і технічних засобів (здатних реалізовувати тільки формальні процедури) за необхідності з’являється проміжний рівень неформальних процедур, які приводяться в дію людиною [7].

Виконавцями процедур є IT-фахівці, співробітники відділів інформаційної безпеки, користувачі і інші співробітники, що пов’язані з інформаційним захистом.

Управління персоналом включає підбір персоналу, прийом на роботу, звільнення, поточний контроль і ін. Кожна з перерахованих дій має відношення до безпеки. При підборі працівників слід перевіряти минуле кандидатів, їх рекомендації, в деяких випадках потрібна додаткова перевірка професійних сертифікатів, кредитної історії, записів в базах даних про злочинців, інші більш ретельні перевірки [1].

При управлінні персоналом слід дотримуватися кількох загальновизнаних принципів.

Розмежування обов’язків переслідує кілька цілей: по-перше, це сприяє підвищенню продуктивності за рахунок спеціалізації, по-друге, усуває непотрібне дублювання, а по-третє (що важливо для безпеки), не дає концентрувати занадто багато повноважень в одних руках. У деяких, особливо критичних випадках, таке розмежування вводиться для того, щоб якась дія могла бути виконана лише за участю двох (або більше) осіб. Приклад такої процедури – доступ до банківського сейфу, який відкривається двома ключами: ключем власника вмісту комірки і ключем представника банку.

Правило обов’язкової відпустки, крім турботи про здоров’я співробітника, дає можливість в його відсутність ґрунтовно перевірити, чи немає порушень в його роботі (однією з непрямих ознак цього може служити зникнення певної проблеми одночасно з його виходом у відпустку), а також чи не використовує деякий зловмисник його обліковий запис (доказом цього служать записи в журналі реєстрації подій, пов’язані з обліковим записом співробітника, після його виходу у відпустку).

Принцип мінімально необхідного рівня привілеїв означає, що кожен співробітник повинен мати тільки той тип доступу і тільки до тих ресурсів, які йому необхідні для виконання його службових обов’язків.

Принцип безперервного навчання правилам безпеки. Ознайомлення з політикою безпеки підприємства при поступленні на роботу повинно доповнюватися регулярними роз’ясненнями всіх внесених до неї змін; необхідно донести до співробітників важливість забезпечення безпеки і пояснити, що в зв’язку з цим очікується від них [7].

Засоби безпеки технічного рівня. Технічні засоби і методи можна розділити на програмні, апаратні та програмно-апаратні. Програмні засоби включають захисні інструменти операційних систем (підсистеми автентифікації та авторизації користувачів, засоби управління доступом, аудит та ін.) і прикладні програми, призначені для вирішення завдань безпеки (системи виявлення та запобігання вторгнень, антивірусні засоби, проксі-сервери).

Прикладом апаратних засобів, що спеціалізуються на інформаційному захисті, є джерела безперебійного живлення, генератори напруги, засоби контролю доступу в приміщення і ін. До апаратно-програмних засобів відносяться, наприклад, деякі аналізатори мережевого трафіку і міжмережеві екрани. І хоча даний рівень засобів називається технічним, до нього також відносять математичні

методи (методи криптографії), алгоритми (евристичний алгоритм розрахунку часу обороту в протоколі TCP), абстрактні моделі (моделі контролю доступу) і т. п.

В роботі [11] відзначається : “Основні стандарти у сфері управління інцидентами інформаційної безпеки, які важливо знати спеціалістам:

- ISO 27002 (A 13)
- ISO 27035
- COBIT5 Enabling Processes (див. процесси DSS 02, DSS 03)
- ITIL (див.. Service operation: Event management, Incident management, Problem management) / аналогічні процеси ISO 20000
- NIST SP 800-61 / NIST SP 800-86
- NIST SP 800-53 (Security control: «Incident Response»)” [11].

Але оскільки майже усі стандарти у сфері інформаційної безпеки грунтуються на стандарті 27000, отже логічно будет спочатку трохи розглянути його.

Серія стандартів з менеджменту (управління) інформаційної безпеки ISO / IEC 27000 розробляється технічним комітетом ISO / IEC JTC 1 підкомітетом SC 27. Система менеджменту інформаційної безпеки (СМІБ) містить в собі вимоги щодо реалізації та вдосконалення систем управління захистом інформації і грунтується на моделі PDCA (Plan-Do-Check-Act):

• створення - ідентифікація активів, менеджмент ризиків;

• впровадження - етап реалізації відповідних заходів з управління безпекою;

• перевірка - моніторинг і аналіз;

• дія - підтримання в робочому стані і поліпшення.

Виходячи з цього видно, що крім розробки правил управління і забезпечення безпеки, не менш важливо забезпечити циклічність всіх процесів з управління безпекою, щоб всі процедури послідовно проходили етапи моделі PDCA. Саме це говорить про відповідність системи управління стандарту ISO 27001 і свідчить про готовність до сертифікації СМІБ.

Виконання вимог стандарту ISO / IEC 27001 головним чином дозволяє мінімізувати ризики втрат активів підприємства / організації, а отже скоротити фінансові втрати. Стандарт ISO / IEC 27001 призначений для сертифікації систем інформаційної безпеки.

Сертифікація системи менеджменту інформаційною безпекою (сертифікація СМІБ) - це ефективне управління бізнес-процесами підприємства / організації,

інформаційними ризиками, а також свідоцтво про стійкою, що розвивається і надійної компанії, що в свою чергу дає позитивне ставлення бізнес-партнерів. СМІБ відповідно до стандарту ISO / IEC 27001 - це частина загальної системи (рис. 1.4) менеджменту компанії [10].

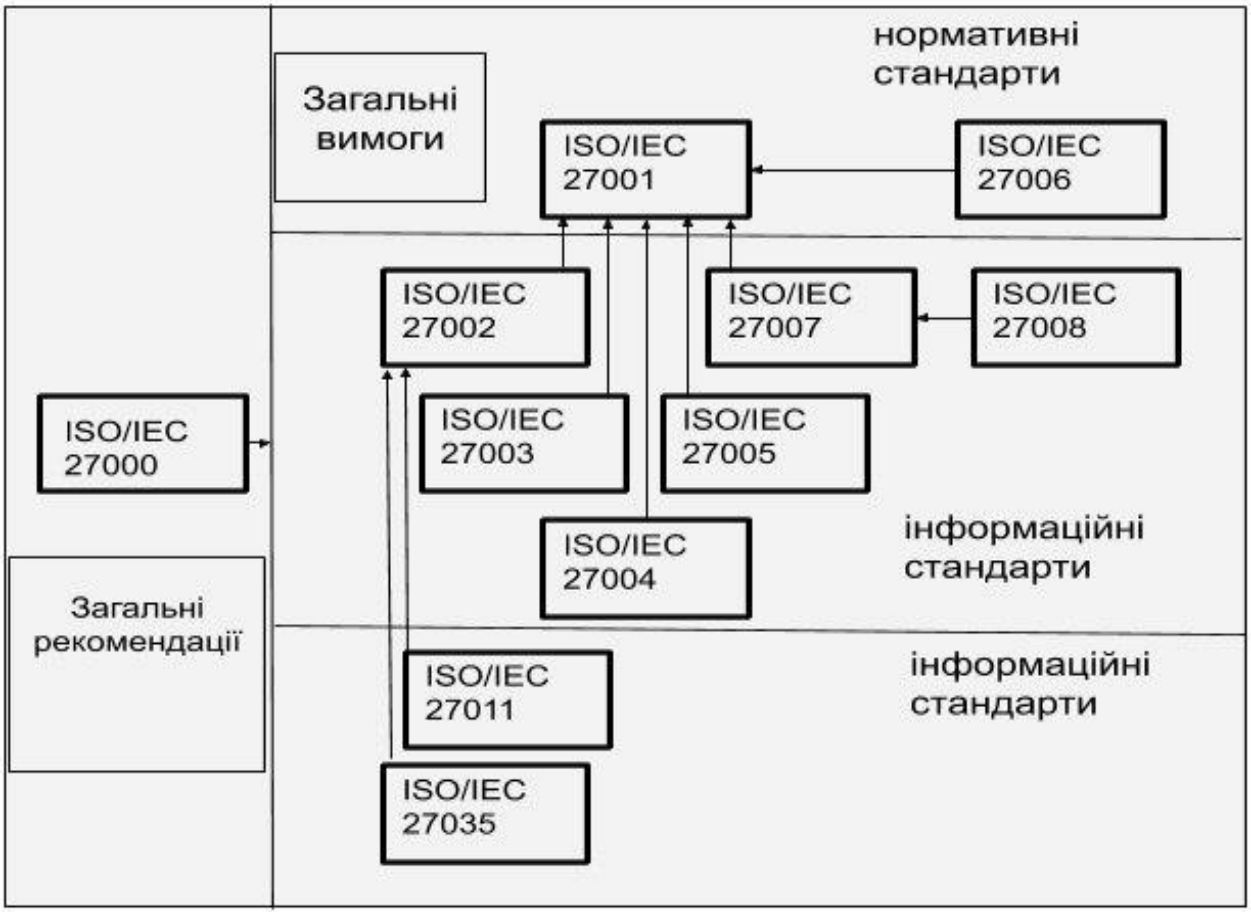

Рис. 1.4. Взаємозв’язок між стандартами ISO

Таблиця 1.1.

Сімейство стандартів ISO 27000

ISO / IEC 27001	Information security management systems. Requirements - Система менеджменту інформаційною безпекою. Вимоги.
ISO / IEC 27000	Information security management systems. Overview and vocabulary - Система менеджменту інформаційної безпеки. Огляд і термінологія.
ISO / IEC 27002	Code of practice for information security management - Практичні правила щодо управління інформаційною безпекою.
ISO / IEC 27003	Information Security Management Systems Implementation Guidance - Керівництво по впровадженню системи менеджменту інформаційною безпекою.
ISO / IEC 27004	Information security management. Measurement - Вимірювання ефективності системи менеджменту інформаційною безпекою.
ISO / IEC 27005	Information security risk management - Управління ризиками інформаційної безпеки.
ISO / IEC 27006	Requirements for bodies providing audit and certification of information security management systems - Вимоги до органів аудиту і сертифікації систем менеджменту інформаційною безпекою.
ISO / IEC 27007	Guidelines for Information Security Management Systems auditing (FCD) - Керівництво для аудиту СМІБ.
ISO / IEC 27008	Guidance for auditors on ISMS controls (DRAFT) - Керівництво по аудиту механізмів контролю СМІБ.
ISO / IEC 27011	Information security management guidelines for telecommunications organizations based on ISO / IEC 27002 - Керівництво з управління інформаційною безпекою для телекомунікацій на основі ISO / IEC 27002.
ISO / IEC 27799	Information security management in health using ISO / IEC 27002 - Керівництво з управління інформаційною безпекою для організацій охорони здоров'я на основі ISO / IEC 27002

Область застосування ISO / IEC 27001: Міжнародний Стандарт встановлює вимоги дорозробці, впровадженню, функціонуванню, моніторингу, аналізу, забезпечення іполіпшенню формалізованої системи менеджменту інформаційної безпеки(СМІБ) в контексті з урахуванням всіх бізнес-ризиків організації. він встановлюєвимоги до застосування засобів управління інформаційної безпеки,адаптованих під потреби кожної організації або якихось її частин. Міжнародний Стандарт може бути використаний усіма організаціями поза, залежно від типу, розміру і характеру бізнесу.

Призначення: ISO / IEC 27001 містить нормативні вимоги до розробки тафункціонуванню СМІБ, включаючи набір засобів управління і зниження ризиків,пов'язаних з інформаційними активами, які організація хотіла б захистити застосуванням СМІБ. Відповідність СМІБ організації може бути перевірено і підтверджена сертифікатом. В ході реалізації СМІБ для виконання вимоги повинні

бути вибрані відповідні завдання управління і засоби управління з Додатку А (ISO / IEC 27001). Завдання управління і засоби управління, наведені в А.1 (ISO / IEC 27001) взяті безпосередньо і повністю відповідають тим, що наведені в розділах 5 - 18 стандарту ISO / IEC 27002.

Область застосування ISO / IEC 27002: Міжнародний Стандарт містить перелік загальноприйнятих завдань управління і визнаних кращих засобів управління, які повинні використовуватися як керівництво щодо застосування при виборі та впровадженні засобів управління для забезпечення інформаційної безпеки.

Призначення: ISO / IEC 27002 містить рекомендації щодо впровадження засобів управління інформаційною безпекою. Саме розділи з 5 по 18 дають відповідні рекомендації щодо впровадження та кращим практикам для підтримки засобів управління, зазначених в розділах А.5 - А.18 ISO / IEC 27001.

Область застосування ISO / IEC 27003: Міжнародний Стандарт містить практичні рекомендації щодо впровадження та додаткову інформацію по розробці, впровадженню, функціонуванню, моніторингу, аналізу, забезпечення і поліпшення СМІБ відповідно до ISO / IEC 27001.

Призначення: ISO / IEC 27003 базується на процесно-орієнтованому підході до успішного впровадження СМІБ відповідно до ISO / IEC 27001.

Область застосування ISO / IEC 27004: Міжнародний Стандарт дає рекомендації по розробці та використанню вимірювань для оцінки результативності СМІБ, виконання задач управління і застосовуваних для забезпечення інформаційної безпеки засобів управління, заданих в ISO / IEC 27001.Призначення: ISO / IEC 27004 пропонує систему вимірювань, що дозволяє оцінити результативність СМІБ, яка повинна вимірюватися відповідно ISO / IEC 27001.

Область застосування ISO / IEC 27005: Міжнародний Стандарт містить рекомендації по менеджменту ризиків інформаційної безпеки. Підхід, прийнятий в цьому Міжнародному Стандарті, забезпечує реалізацію концепції, представленої висок / IEC 27001.

Призначення: ISO / IEC 27005 служить керівництвом по впровадженню процесно орієнтованого підходу до менеджменту ризику, щоб допомогти в реалізації і виконанні вимог до менеджменту ризиків інформаційної безпеки, встановлених в ISO / IEC 27001.

Область застосування ISO / IEC 27007: Міжнародний Стандарт містить рекомендації з проведення аудитів СМІБ, а також керівництво щодо забезпечення компетентності аудиторів систем менеджменту інформаційної безпеки на додаток до вказівкам, що містяться в ISO 19011, які застосовні до систем менеджменту в цілому [7].

Призначення: ISO / IEC 27007 містить рекомендації організаціям, яким необхідно проводити внутрішні або зовнішні аудити СМІБ або керувати програмою аудиту СМІБ відповідно до вимог, встановлених в ISO / IEC 27001.

Область застосування ISO / IEC 27008: Технічний Звіт дає рекомендації з перевірки впровадження та виконання коштів управління, включаючи перевірку технічної відповідності засобів управління інформаційних систем, відповідно до встановлених в організації стандартів інформаційної безпеки.

Призначення: Технічний Звіт наголошує на перевірках засобів управління інформаційною безпекою, включаючи перевірки технічної відповідності, відповідно до стандарту забезпечення інформаційної безпеки, який встановлений в організації. Він не спрямований на забезпечення будь-яких конкретних рекомендацій з перевірки відповідності в плані вимірювань, оцінки ризику або аудиту СМІБ, які містяться в ISO / IEC 27004, ISO / IEC 27005 або ISO / IEC 27007 відповідно. Технічний Звіт не орієнтований на аудити систем менеджменту.

Область застосування ISO/IEC 27013: Міжнародний Стандарт надає керівні вказівки щодо інтегрованого впровадження стандартів ISO / IEC 27001 та ISO / IEC 20000-1 в організаціях, що прагнуть до:

a) впровадження ISO / IEC 27001 при вже запровадженому ISO / IEC 20000-1 або навпаки;

b) спільного впровадження ISO / IEC 27001 та ISO / IEC 20000-1;

c) узгодження впроваджених систем менеджменту відповідно до ISO / IEC 27001 та ISO / IEC 20000-1.

Призначення: Забезпечити організаціям краще розуміння характеристик, схожості і відмінностей ISO / IEC 27001 та ISO / IEC 20000-1, щоб допомогти при плануванні інтеграції систем менеджменту, які відповідають цим двом Міжнародних Стандартів.

Область застосування ISO/IEC 27014: Міжнародний Стандарт містить принципи і процеси управління інформаційною безпекою, за допомогою яких

організація може оцінювати, направляти і контролювати менеджмент інформаційної безпеки [8].

Призначення: Інформаційна безпека стає ключовим фактором для організацій. Не тільки посилення нормативних вимог, але також і збій в функціонуванні засобів забезпечення інформаційної безпеки в організації може мати прямий вплив на репутацію організації. Таким чином, від керуючих органів, в рамках їх спільної відповідальності, все більше потрібно приділяти увагу інформаційної безпеки, щоб гарантувати досягнення цілей організації.

Область застосування ISO/IEC 27016: Технічний Звіт містить методологію, що дозволяє організаціям кращим чином зрозуміти з економічної точки зору,яким чином більш точно визначити цінність виявлених інформаційних активів,оцінити потенційні ризики для цих інформаційних активів, оцінити внесок,який вносять засоби захисту в цінність цих інформаційних активів, а також визначити оптимальний рівень ресурсів, який необхідно задіяти при захисті цих інформаційних активів.

Призначення: Технічний Звіт доповнює сімейство стандартів СМІБ, додаючи економічний аспект в захисті інформаційних активів організації в контексті більш широкого соціального середовища, в якій діє організація, і надає рекомендації, як враховувати економічні аспекти інформаційної безпеки, на основі моделей і прикладів [12].

Тепер по стандарту ISO 27035.В цілому політики інформаційної безпеки або засоби управління самі по собі не гарантують повний захист інформації, інформаційних систем, послуг або мереж. Після впровадження засобів управління існує ймовірність, що залишилися уразливості знижують ефективність ІБ і, таким чином, сприяють виникненню інцидентів ІБ. Потенційно це може мати непрямий і прямий несприятливий вплив на ділову активність організації.

Більш того, неминуче будуть виникати нові загрози, які було визначено раніше. Відсутність достатньої підготовки організації по боротьбі з такими інцидентами робить будь-яку реакцію менш ефективною і збільшує ступінь можливого негативного впливу на діяльність організації. Тому для будь-якої організації важливо серйозно ставиться до ІБ і мати структурований і спланований підхід до:

- виявлення, звітності та оцінки інцидентів ІБ;

- реагування на інциденти ІБ, включаючи активізацію відповідних засобів управління для запобігання, мінімізації та відновлення після негативного впливу (наприклад, при підтримці зон антикризового управління);

- звітності про уразливість ІБ, які раніше не були використані і не стали причиною подій або можливих інцидентів ІБ, а також оцінці і боротьби з ними відповідним чином;

- вивчення інцидентів і вразливостей ІБ, впровадження превентивних засобів управління і вдосконалення загального підходу до управління інцидентами ІБ.

1. Область застосування

Цей стандарт забезпечує структурований і плановий підхід до:

- виявлення, звітності та оцінки інцидентів ІБ;

- реагування та управління інцидентами ІБ;

- виявлення, оцінки та управління уразливими ІБ;

- постійного вдосконалення ІБ і управління інцидентами з урахуванням результатів управління інцидентами і уразливими ІБ.

Цей стандарт це керівництво з управління інцидентами ІБ для великих і середніх організацій. Малі організації, в залежності від їх розміру, типу діяльності і ситуації з ризиками ІБ, можуть використовувати з базового набору, описаного в цьому стандарті, необхідні їм документи, процеси і процедури. Він також надає керівництво для зовнішніх організацій, що надають послуги з управління інцидентами ІБ.

2. Нормативні посилання

У цьому стандарті є посилання на такі нормативні документи:

- ISO / IEC 27000 Інформаційні технології. Методи захисту. Системи управління ІБ. Огляд і словник

- ISO / IEC 27001 інформаційне технології. Методи захисту. Системи управління ІБ. вимоги

- ISO / IEC 27002 інформаційне технологія. Методи захисту. Практичні правила управління ІБ

- ISO / IEC 27005 Інформаційні технології. Методи захисту. Управління ризиками ІБ

3. Терміни, визначення та скорочення

У цьому документі використано терміни по ISO / IEC 27000, а також такі терміни та визначення:

- експертиза ІБ: застосування методів дослідження і аналізу для виявлення, реєстрації та перевірки інцидентів ІБ.

- група реагування на інциденти ІБ (ГРІІБ): група кваліфікованих і довірених співробітників організації, яка обробляє інциденти ІБ під час їх життєвого циклу.

Примітка: ГРІІБ - це посадові обов'язки, які охоплюють процес інцидентів ІБ і зосереджені головним чином на інциденти, пов'язані з інформаційними технологіями. Інші загальні обов'язки (з аналогічними абревіатурами) в рамках обробки інцидентів можуть мати дещо інші масштаб і цілі. Наступні використовувані абревіатури мають сенс аналогічний ГРІІБ.

CERT (Computer Emergency Response Team) - служба реагування на комп'ютерні інциденти в основному зосереджена на інциденти в інформаційно-комунікаційних технологіях (далі - ІКТ).

CSIRT (Computer Security Incident Response Team) - служба реагування на інциденти комп'ютерної безпеки - це служба, яка відповідає за отримання, перевірку та реагування на повідомлення про інциденти комп'ютерної безпеки і їх активність. Ці послуги зазвичай виконуються для певних замовників, якими можуть бути головна компанія корпорації, державні організації, освітні організації, регіони або країни, дослідницькі мережі або комерційні клієнти.

- подія ІБ: ідентифікований випадок стану системи, послуги або мережі, що вказує на можливе порушення політики безпеки або на відмову засобів захисту, або на раніше невідому ситуацію, яка може бути істотною для безпеки. [ISO / IEC 27000]

- інцидент ІБ: одинична подія або ряд небажаних або непередбачуваних подій ІБ, через які велика ймовірність компрометації бізнес-операцій і загрози ІБ. [ISO / IEC 27000]

Виникнення події ІБ не обов'язково означає, що спроба була успішною або що надала будь-який вплив на конфіденційність, цілісність і / або доступність, тобто в повному обсязі події ІБ класифікуються як інциденти ІБ.

Інциденти ІБ можуть бути навмисними (наприклад, шкідливі програми та злочинні дії) або випадковими (наприклад, людські помилки або стихійні лиха), а також створюватися технічними або фізичними засобами. Їх наслідками можуть бути несанкціоноване розголошення, модифікація, знищення або недоступність інформації, або пошкодження чи крадіжку активів, що містять інформацію.

Далі на схемі взаємозв'язку понять (рис. 1.5) розглянемо місце інциденту в ІБ [14].

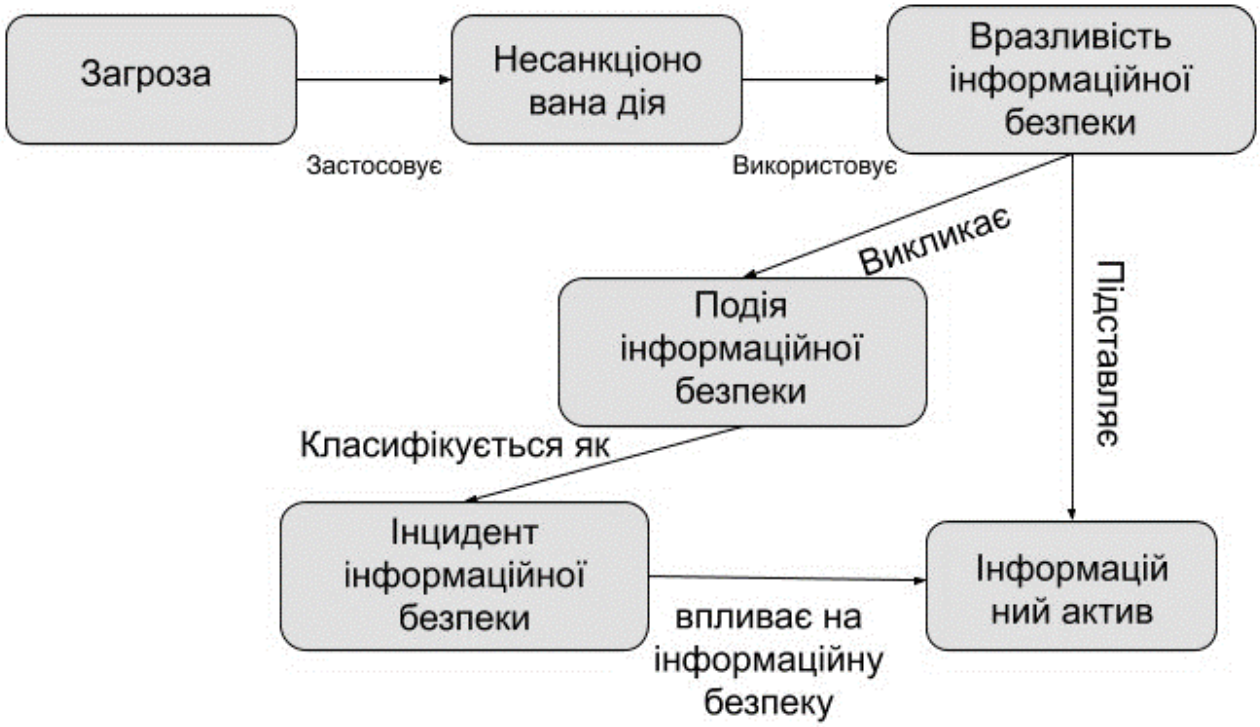

Рис. 1.5. Схема взаємозв'язку понять

Розглянуті у першому розділі основні характеристики інформаційної безпеки підприємтсва та основні вимоги стандартів з управління інформаційною безпекою, та управління інцидентами надають основне розуміння або мінімальний варіант забезпечення безпеки для підприємства на більш меньш законних умовах, також впроваджуючи вже цей мінімум вимог дає можливість їх покращення та розробку нових положенньь, но основі приблизно такій самій.

Таким чином необхідно врахувати усе вище перераховане з позиції системи забезпечення інформаційної безпеки підприємства, оскільки системи бувають різного характеру та розміру, але функціонують завдяки взаємозв`язкам.

2 АНАЛІЗ ОРГАНІЗАЦІЇ УПРАВЛІННЯ ІНЦИДЕНТАМИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Впровадження системи забезпечення інформаційної безпеки

Вже давно було розроблено концепції розрізнення [15], на яких і будується даний розділ розрізненням системи забезпечення безпеки та системи забезпечення. Одразу вважаю необхідним визначити мету за якої з`явилась дана система і почала функціонувати також про її розвиток і її стан на Україні за останні роки.

Останнім часом використання досягнень у сфері інформаційних технологій дуже часто стає невідє`мною складовою на підприємствах та у країнах на початку нового 20го століття, яке можна вже охарактеризувати з деякою глобалізацією економічних та політичних складових держав. На Україні не так вже давно було обрано шлях інтеграції до ЄС, а як відомо Європа - це список країн у яких активно проходять процеси з устрою інформаційного суспільства, а отже і в Україні стає важливим питання ефективного та належного забезпечення інформаційної безпеки навіть на державному рівні.

Оскільки технології розвиваються, інформація стає найдорожчим на найціннішим ресурсом глобального характеру. Навіть можна так сказати, що на сьогоднішній день потенціал суспільства або рівень розвитку можна визначати об`ємом інформаційних ресурсів, а також ступінню розвитку самої інформаційної інфраструктури. За останній час зростає кільскість інформації, споживання, джерел появи, а отже сама інформація завжди у процесі постійного ускладнення, та удосконалення. Якщо усе розглядати під таким кутом як вище написано, то розвиток злочинності у цій сфері також буде розвиватися, під злочиністтю розглядаються такі фактори як: недостовірність, шкідливість, несвоєчасність, шпигунство, та комп`ютерна злочинність та ін. Сама за таких обставин у головному законі України, у конституції вказано що забезпечення ІБ відноситься до одних із найважливіших функцій на території держави. Якщо ознайомитись з Доктриною ІБ України, то у сучасних умовах все більше уваги отримує інформаційна ланка яка також стала одним із головних елементів національної безпеки. Усе з чого складається інформаційна сфера, тобто Інформаційний простір, інформаційна інфраструктура, інформаційні ресурси та інформаційні технології мають досить

великий вплив на соціально-економічний, науково-технічний та культурний ріст. [9].

А отже ІБ стає обов`язковим пунктом усіх галузей національної безпеки. Так само інформаційна безпека - це необхідна, самостійна складова забезпечення національної безпеки. Як один із висновків один стає досить прозорим, а саме, щоб забезпечити стабільний та міцний розвиток та ріст на Україні в основних галузях та з дотриманням законів, має за собою важливий та необхідний крок забезпечення достатнього рівня ІБ. Україна має досить гарне геополітичне розташування, також велику історичну, багату духовну спадщину, слідуючи основним моральним поняттям розвитку та самовдосконалення, Україна може стати достатньо сильною державою в більшості галузей, це призведе до повноправності у європейській спілці, та певної сили та впливовості, що дає змогу посісти одне з перших місць у глобалізованому світі. Зміст Доктрини ІБ України дає чітко зрозуміти що головною ціллю її впровадження, буде створити захищений національний інформаційний простір. Забезпечення інформаційної безпеки України має здійснюватися за такими принципами [6]:

• свобода збирання, зберігання, використання та поширення інформації;

• достовірність, повнота та неупередженість інформації;

• обмеження доступу до інформації виключно на підставі закону;

• гармонізація особистих, суспільних і державних інтересів;

• запобігання правопорушенням в інформаційній сфері;

• економічна доцільність;

• гармонізація українського законодавства в інформаційній сфері з міжнародним;

• пріоритетність національної інформаційної продукції.

Основні задачі забезпечення інформаційної безпеки підприємства на Україні:

• виявлення, оцінка та прогнозування джерел загроз інформаційній безпеці;

• розробка державної політики забезпечення інформаційної безпеки та комплексу заходів і механізмів її реалізації;

• створення нормативно-правових засад забезпечення інформаційної безпеки, координація діяльності органів державної влади та управління, установ та підприємств по реалізації політики інформаційної безпеки;

• розвиток системи забезпечення інформаційної безпеки, вдосконалення її організації, форм, методів і засобів запобігання загрозам інформаційній безпеці та

ліквідації наслідків її порушення;

• забезпечення участі України в процесах створення і використання глобальних інформаційних мереж та систем [5].

Поняття системи забезпечення інформаційної безпеки

У держави не буде гармонійних та перспективних умов розвитку без достатньь надійної системи забезпечення інформаційної безпки, а це вже має свій вплив на національну безпеку. А оскільки основною метою є забезпезпечення надійності існування особи, суспільства і держави в інформаційному просторі, якщо це розглядати з позиції основної мети системи забезпечення інформаційної безпеки [6].

Система забезпечення інформаційної безпеки України (СЗІБ) інує та вдосконалюється дотримуючись законів України та основниї нормативно-правових актів, які вже існують в інформаційній ланці. Головними в данній сфері є органи, нормативи та стандарти забезпечення інформаційної безпеки, які розглядаються на адміністративно-правовому, огранізаційно-управлінському, інформаційно-аналітичному ріні, дотримуючись цих засобів можливо створити міцну систему державного керування [6].

Створення СЗІБ повинно проходити після усвоєння інформації про певний “баланс інтересів” основних функцій системи державного управління в ІБ.

Окремо треба відмітити, те що на Україні незалежній тобто за останні роки, поки що тільки існує мала база основних положеннь у сфері інформаційної безпеки. Тим самим можна сказати про невеликий перелік номративно-правових актів, у яких обгрунтовані головні можливості держ. органів у галузі інформації. Головою країни застосовуються певні міри за яких відбувається розвиток системи управління інфомраційною галуззю.

В той самий час роботоспроможність цієї системи не завершується тільки переліком основних положеннь у нормативній базі. А отже як факт не можливо сказати про досконалість головних моментів у системі забезпечення інформаційної безпеки. А саме чому, зараз і розглянемо. В першу чергу це не існує чітко визначених рамок у СЗІБ, також слабка позиція національної політики країни, що призводить до неповної картини безпеки інформації, але існує Доктрина ІБ, вона допомагає і нібито перекриває ці недостатки і допомагає розвиватись основним концепціям у сфері ІБ на території України. Але з плином часу прогалини у

законодавстві та нормативних актах регулювання, в цілому починає залишати свій негативний відбиток на керування процесами у державі [6].

Основними засадами які розглядаються на благо росту та вдосконалення положення на Україні на даний момент у СЗІБ являються: Конституція України, Закон України "Про основи національної безпеки України", Доктрина, стандарти ГОСТи серії 27000 і йому подібні. Завдяки розвитку цієї галузі в інших країнах можливим стає переймати досвід, оскільки ця сфера виходить на перший рівень важливості та цінності у основних сферах діяльності та розвитку нації, головне брати приклади з урахуванням прав на свободу людини на отримання та розповсюдження інформації. Так само вплив йде і на окремі галузі, завдяки не чітко окресленим нормативним актами та правовим врегулюванням додаються багато проблем, а це в свою чергу несе свій негативний тиск на їх формування і якість даної вже застосованої бази по основним пунктам забезпечення національної безпеки України у рамках інформаційної галузі [7].

Безперечно, можуть бути тривалі дискусії щодо конкретного терміну, і можна запропонувати багато варіантів, але вони мають сенс лише після визначення основ формування та функціонування СЗІБ [6].

Основами створення та роботи системи захисту інформації є:

- повне визначення поняття інформаційної безпеки та її складових, ідейно-концептуальна консолідація в концепціях, доктринах, програмах, планах та інших документах;
- Розробка та функціонування оптимальної структури системи інформаційної безпеки, аналіз функціонування окремих її елементів, організація функціонування цієї системи в цілому;
- розробка єдиного методологічного підходу, а також розробка та прийняття єдиного, узгодженого та затвердженого законодавства про інформаційну безпеку;
- Створити чіткий механізм координації діяльності елементів системи захисту інформації на всіх рівнях влади;
- Навчайте та надайте найкращим професіоналам усі компоненти підсистеми інформаційної безпеки.

Враховуючи ці основи, ми можемо говорити про їх систематичну взаємодію, яка забезпечить створення та функціонування чіткого та надійного СЗІБ.

За основними ознаками навчання можна виділити основні функції системи інформаційної безпеки України.

1. Створення та підтримка діяльності урядових та неурядових організацій та органів - елементів системи інформаційної безпеки, зокрема:

* Розробка адміністративно-правових основ структури та функціонування системи інформаційної безпеки (принципи інформаційної безпеки, організаційна та функціональна структура системи);

* Систематичне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративне, логістичне, кадрове, підтримка ресурсів усієї системи державного управління.

2. Управління інформаційною безпекою - знання цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, внутрішні та зовнішні фактори, що впливають на стан інформаційної безпеки:

* Розробити на основі теорії інформаційної безпеки конкретні плани та технології для забезпечення інформаційної безпеки відповідно до вимог різних державних рівнів;

* Впровадження прогнозування, планування, організації, регулювання та контролю всієї системи захисту інформації та окремих її елементів;

* Оцінка ефективності заходів, вартості заходів інформаційної безпеки.

3. Реалізація планових та оперативних заходів інформаційної безпеки:

* Визначити інтереси державної адміністрації у сфері інформації та її пріоритет відповідно до Державної інформаційної політики;

* Діагностика загроз та загроз, виявлення джерел їх виникнення та прогнозування можливих наслідків у разі їх появи з розробкою відповідних профілактичних заходів.

4. Міжнародне співробітництво в галузі інформаційної безпеки:

* Розробити правову базу для інформаційних відносин між державами та їх взаємодії у сфері інформаційної безпеки;

* Знання про створення та створення нових двосторонніх та багатосторонніх структур (організацій), діяльність яких спрямована на вирішення проблем інформаційної безпеки з урахуванням національних інтересів України;

* Участь у роботі підрозділів управління, керівництва та підтримки цих структур (організацій), спільне виконання планових та оперативних заходів.

Звичайно, перелік функцій не є вичерпним, але в той же час можна говорити про формування конкретної підсистеми, мета якої сумісна із загальним

призначенням системи національної безпеки. Важливо проаналізувати зміст та призначення системи захисту інформації в контексті обговорюваних питань.

Інформаційна безпека досягається цілеспрямованими діями державного сектору для запобігання можливого порушення їх нормальної діяльності загрозами та небезпеками.

Єдиної оптимальної структури захисту інформації не існує, так як кожна організація-учасник інформаційних процесів має свій власний відрізняється від інших набір вимог, проблем і пріоритетів, продиктованих об'єктивними економічними, виробничими, соціальними умовами функціонування даного підприємства. Тому основоположним моментом створення на підприємстві системи забезпечення інформаційної безпеки є розробка і реалізація унікальної, максимально адаптованої до конкретних умов політики інформаційної безпеки [12].

Здійснюючи проектування ефективної системи інформаційної безпеки або її модернізацію, слід керуватися існуючої концептуальної схемою ефективної системи інформаційної безпеки, представленої на малюнку

1.Згідно до позначених етапів схеми, виконуються конкретні дії, які в сукупності представляють собою цілісну системну взаємодію технічних, технологічних, організаційних, економічних та правових заходів, що забезпечують необхідний рівень інформаційної безпеки.

1) Діагностичне обстеження / аудит системи інформаційної безпеки. Для побудови ефективної системи інформаційної безпеки, вибір і впровадження адекватних технічних засобів захисту повинен передувати аналізом загроз, вразливостей інформаційної системи і на їх основі - аналізом ризиків інформаційної безпеки. вибір програмно-апаратного забезпечення захисту та проектування систем інформаційної безпеки грунтується на результатах такого аналізу з урахуванням економічної оцінки співвідношення «вартість контрзаходів щодо зниження ризиків / можливі втрати промислового підприємства від інцидентів інформаційної безпеки ».

Рис. 2.1 Схема вимог до забезпечення інформаційної безпеки підприємства.

Схема вимог до забезпечення інформаційної безпеки підприємства визначає, що її побудову важливо починати з проведення комплексної діагностики основних бізнес-процесів підприємства та його інформаційної системи в цілому [15]. Діагностіка системи інформаційної безпеки підприємства дасть можливість визначити рівень безпеки інформаційно-технологічних ресурсів промислового підприємства і співвіднести їх з ставляться відповідно до параметрів конфіденційності, доступності та цілісності ресурсів інформаційної системи. Також, проведення комплексної діагностики дозволить виявити можливі і ризики і визначити заходи щодо протистояння несанкціонованому доступу та впливу на інформацію підприємства.

2.2 Методичні підходи до організації управління інцидентами в системі забезпечення інформаційної безпеки

Як управляти інцидентами інформаційної безпеки. Які конкретно дії необхідно виконати для розробки процедури управління інцидентами інформаційної безпеки.

Для початку необхідно, щоб процес розробки процедури (як і всіх процедур в компанії) був ініційований її керівництвом. Як правило, процедура управління інцидентами розробляється в рамках загальної системи управління інформаційною безпекою, тому важливою є позиція керівництва з питання її створення і функціонування. На даному етапі важливо, щоб всі співробітники компанії розуміли, що забезпечення інформаційної безпеки в цілому і управління інцидентами зокрема є основними бізнес-цілями компанії [14].

Потім слід розробити необхідні нормативні документи з управління інцидентами. Як правило, такі документи повинні описувати:

- визначення інциденту інформаційної безпеки, перелік подій, які є інцидентами (що в компанії є інцидентом);
- порядок оповіщення відповідальної особи про виникнення інциденту (необхідно визначити формат звіту, а також відобразити контактну інформацію осіб, яких слід повідомляти про інцидент);
- порядок усунення наслідків і причин інциденту;
- порядок розслідування інциденту (визначення причин інциденту, винних у виникненні інциденту, порядок збору та збереження доказів);
- внесення дисциплінарних стягнень;
- реалізація необхідних коригувальних і превентивних заходів [15].

Визначення переліку подій, які є інцидентами, - важливий етап розробки процедури управління інцидентами. Слід розуміти, що всі події, які не ввійдуть до зазначеного переліку, будуть розглядатися як штатні (навіть якщо вони несуть загрозу інформаційній безпеці). Зокрема, інцидентами інформаційної безпеки можуть бути:

- отказ в обслуживании сервисов, средств обработки информации, оборудования;
- нарушение конфиденциальности и целостности ценной информации;

- несоблюдение требований к информационной безопасности, принятых в компании (нарушение правил обработки информации);
- незаконный мониторинг информационной системы;
- вредоносные программы;
- компрометация информационной системы (например, разглашение пароля пользователя) [14].

Як приклад інцидентів можна привести такі події, як неавторизоване зміна даних на сайті компанії, залишення комп'ютера незаблокованим без нагляду, пересилання конфіденційної інформації за допомогою корпоративної або особистої пошти. У загальному випадку інцидент інформаційної безпеки визначається як одиничне, небажане або несподівана подія інформаційної безпеки (або сукупність таких подій), яке може скомпрометувати бізнес-процеси компанії або загрожує її інформаційної безпеки.

Визначальним елементом створення будь-якої системи є її мета. Отже, очевидним є розгляд даного компоненту і при створенні системи забезпечення інформаційної безпеки підприємства.

Виходячи з наведеного, мета функціонування системи забезпечення інформаційної безпеки полягає в організації управління системою інформаційної безпеки через ефективне функціонування самої системи її забезпечення. У більш загальному плані мета полягає у створенні необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життя і діяльності громадянина, суспільства й держави.
Ефективність системи державного управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи державного управління цими процесами призводять до непоправних збитків суспільству й державі. Наприклад, відомо, що втрати економіки Німеччини від індустріального шпигунства перевищують 20 млрд євро на рік, втрата торгових і технічних секретів США (за неофіційними даними) [10] обійшлась американським компаніям у 1992 році в 100 млрд доларів.

Для досягнення поставленої мети на систему забезпечення інформаційної безпеки покладаються певні завдання.

Головним завданням системи забезпечення інформаційної безпеки України є створення умов для організації управління системою інформаційної безпеки.

До основних завдань системи забезпечення інформаційної безпеки належать:

- створення умов для забезпечення інформаційного суверенітету України;
- участь у вдосконаленні державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- створення умов для активного залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.
- забезпечення інформаційної безпеки усіх складових елементів системи державного управління;
- забезпечення інформаційно-аналітичного потенціалу країни;
- реалізація державної політики інформаційної безпеки;
- ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки для відпрацювання стратегічних, тактичних і оперативних рішень у сфері державного управління інформаційною безпекою та вироблення механізмів їх реалізації;
- виявлення, попередження і припинення розвідувальної та іншої, спрямованої на нанесення шкоди інформаційній безпеці України, діяльності спеціальних служб, а також окремих осіб чи організацій;
- виявлення, попередження і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи державного управління;

- моніторинг (спостереження, оцінка і прогноз) стану інформаційної безпеки у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні системи державного управління;
- протидія технічному проникненню до інформаційних системи органів державного управління з метою вчинення злочинів, проведення диверсійно-терористичної та розвідувальної діяльності;
- запобігання можливої протиправної та іншої негативної діяльності суб'єктів системи забезпечення національної безпеки зсередини системи їй на шкоду;
- забезпечення збереження державної таємниці;
- організація демократичного цивільного контролю за функціонуванням системи органів державного управління тощо.

Відповідно до окресленої мети і завдань, доцільно визначити функції системи забезпечення інформаційної безпеки підприємства.

Під функціями системи забезпечення інформаційної безпеки розуміється здійснення суб'єктами системи забезпечення інформаційної безпеки підприємства діяльності зі створення умов для оптимального управління системою інформаційної безпеки.

Зазначимо, що погляди щодо функцій даної системи різняться. В роботі [15] відзначається наступне: “Серед основних функцій системи забезпечення інформаційної безпеки в умовах надзвичайної ситуації слід виділити: виявлення і прогнозування загроз життєво важливим інтересам об'єктів інформаційної безпеки, здійснення комплексу оперативних і довгострокових заходів для попередження та нейтралізації загроз; створення та підтримання напоготові сил і засобів забезпечення інформаційної безпеки; управління силами і засобами забезпечення інформаційної безпеки в умовах надзвичайної ситуації; здійснення системи заходів з відновлення нормального функціонування об'єктів інформаційної безпеки у регіонах, які потерпіли внаслідок виникнення надзвичайної ситуації; участь в заходах, покликаних забезпечувати інформаційної безпеку за межами України відповідно до міжнародних договорів та угод, укладених або визнаних українською державою.Аналогічними за своїм змістом є пропоновані функції В.Ю.Богдановичем” [15].

До основних принципів СЗІБ підприємства можна віднести:

1. Принцип комплексності. При створенні захисних систем необхідно припускати ймовірність виникнення всіх можливих загроз для кожної організації,

включаючи канали закритого доступу і використовувані для них засоби захисту. Застосування засобів захисту повинно збігатися з імовірними видами загроз і функціонувати як комплексна система захисту, технічно доповнюючи один одного. Комплексні методи і засоби забезпечення інформаційної безпеки організації є складною системою взаємопов'язаних між собою процесів.

2. Принцип ешелонування є порядок забезпечення інформаційної безпеки організації, при якому всі рубежі захисної системи будуть складатися з послідовно розташованих зон безпеки, найважливіша з яких буде знаходитися всередині всієї системи.

3. Принцип надійності. Стандарт організації забезпечення інформаційної безпеки повинен стосуватися всіх зон безпеки. Всі вони повинні бути равнопрочность, тобто мати однакову ступінь надійного захисту з ймовірністю реальної загрози.

4. Принцип розумної достатності передбачає розумне застосування захисних засобів з прийнятним рівнем безпеки без фанатизму створення абсолютного захисту. Забезпечення організації високоефективної захисною системою передбачає великі матеріальні витрати, тому до вибору систем безпеки потрібно підходити раціонально. Вартість захисної системи не повинна перевищувати розмір можливого збитку і витрати на її функціонування і обслуговування.

5. Принцип безперервності. Робота всіх систем безпеки повинна бути цілодобовою і безперервною [16].

Незважаючи на те, що стандарти прямо рекомендують впроваджувати методики управління інциденту інформаційної безпеки, на практиці впровадження та реалізації цих практик зустрічають безліч складнощів. Окремі процедури управління інциденту не впроваджуються. Цей показник не говорити про те, що система менеджменту інцидентів працюють добре чи погано, це свідчить тільки про те, що існує певна брешемо в системі безпеки.

Управління інциденту інформаційної безпеки засноване на наступних діях:

- Визначення. В організації відсутній методика виявлення і класифікації інцидентів, опис їх основних параметрів, тому співробітники встають перед необхідністю або самостійно визначати критерії події, або ігнорувати його. Вхід в мережу під обліковим записом іншого співробітника, відповідно до стандартів, є інцидентом інформаційної безпеки, але він не буде зафіксований в журналі, так як

співробітники вважають таку поведінку стандартним і дозволеним, особливо в умовах дефіциту кадрових ресурсів;

- Оповіщення про виникнення. Навіть якщо яка-небудь подія може бути визначено згідно з прийнятими в організації методикам або особисту думку співробітника як інцидент, найчастіше в організації не розроблені стандарти і маршрути оповіщення про такі події. Навіть якщо кимось буде виявлено факт копіювання документів, що відносяться до комерційної таємниці, співробітник встане в безвихідь перед питанням, хто саме і в якій формі має бути сповіщений про цей інцидент: його керівник, служба безпеки або інша особа;
- Реєстрація. Ця частина стандартів є найбільш нездійсненним для російських компаній, інциденти не ідентифікуються, відповідно, не фіксуються. Відсутня практика закладу регістрів обліку, в яких би фіксувалися значущі події, що згодом давало б матеріал для їх аналізу і прогнозу можливих атак;
- Усунення причин і наслідків. Будь інцидент викликає певні сліди і наслідки, які, з одного боку, можуть заважати діяльності компанії, з іншого - служать матеріалом для проведення розслідування причин його виникнення. Відсутність регламентів усунення наслідків може привести як до накопичення помилок, так і до повного знищення доказової бази, що дозволяє виявити винуватця сталася ситуації. Будь-які термінові заходи, що вживаються для відновлення стабільності, можуть випадково або навмисно знищити сліди проникнення в базу даних;
- Заходи реагування на інциденти. У ряді випадків виникнення інциденту може зажадати термінових заходів реагування, наприклад, відключення комп'ютера від мережі, припинення передачі інформації, установки контакту з провайдером. Повинні бути визначені органи і посадові особи, відповідальні за розробку механізму реагування і його оперативну реалізацію;
- Розслідування. Повноваження по розслідуванню повинні бути передані з відання IT-служби в компетенцію служб безпеки. В рамках розслідування повинні бути вивчені журнали обліку, проаналізовані дії всіх користувачів і адміністраторів, які мали доступ до систем в період виникнення надзвичайної ситуації. Розслідування повинно стати одним з основних елементів управління інцидентами. На практиці в російських компаніях від реалізації цього етапу відмовляються, обмежуючись усунення наслідків події, що сталася. При необхідності розслідування повинно проводитися із залученням оперативно-слідчих органів;

- Реалізація превентивних заходів. У більшості випадків інциденти не є поодинокими, їх виникнення свідчить про те, що в системі ІБ виникла пролом і аналогічні випадки будуть повторюватися. Щоб уникнути цих ризиків необхідно за результатами розслідування підготувати протокол або акт комісії, в якому визначити, які саме заходи повинні бути застосовані для запобігання аналогічних ситуацій. Крім того, застосовуються певні заходи дисциплінарної відповідальності, передбачені Трудовим кодексом і внутрішніми регламентами;
- Аналітика. Всі події, що порушують регламентовані процеси і можуть бути кваліфіковані як інцидентів інформаційної безпеки, повинні стати основою для аналізу, який допоможе визначити їх характер, проявити системність і виробити рекомендації для вдосконалення системи ІБ, діючу пенсійну систему компанії.

Як будь-яка корпоративна процедура, організація управління інцидентами інформаційної безпеки повинна пройти кілька етапів: від прийняття рішення про його необхідності до впровадження і аудиту. На практиці менеджмент більшості підприємств не усвідомлює необхідності застосування цієї практики захисту інформаційного периметра, тому для виникнення ініціативи про її впровадження часто потрібно аудит систем ІБ зовнішніми консультантами, вироблення ними рекомендацій, які потім будуть реалізовані керівництвом підприємства. Таким чином, початковою точкою для реалізації процедур управління інцидентами ІБ стає рішення виконавчих органів або іноді більш високих ланок системи управління компанії, наприклад, Ради директорів.

Загальне рішення зазвичай приймається в руслі модернізації існуючої системи ІБ. Система управління інцидентами є її основною частиною. На рівні прийняття рішення необхідна його локалізація в загальній парадигмі цілей компанії. Оптимально, якщо функціонування системи ІБ стає однією з бізнес-цілей організації, а якість її роботи підкріплюється встановленням ключових показників ефективності для відповідальних співробітників компанії. Після визначення статусу функціонування системи необхідно перейти до розробки внутрішньої документації, пов'язані з нею відносини в компанії.

Для додання значущості методикам управління інформаційною безпекою вони повинні бути затверджені на рівні виконавчого органу (генерального директора, правління або ради директорів). З даними документа необхідно ознайомити всіх співробітників, що мають відношення до роботи з інформацією, яка існує в електронних формах або на матеріальних носіях.

У структурі документа, який оформлюється у вигляді положення або регламенту, повинні виділятися наступні підрозділи:

1. Визначення подій, визнаних інцидентами стосовно до системи безпеки конкретної компанії. Так, користування зовнішньої електронною поштою може бути порушенням ІБ для державної компанії і рядовою подією;

2. Порядок оповіщення про подію. Повинні бути визначені формат повідомлення (усний, доповідна записка, електронне повідомлення), перелік осіб, які мають бути повідомлені, і дублюючі їх посади в разі їх відсутності, перелік осіб, до яких також доноситься інформація про подію (керівництво компанії), строк повідомлення після отримання інформації про інцидент; перелік заходів щодо усунення наслідків інциденту і порядок їх реалізації;

3. Порядок розслідування, в якому визначаються відповідальні за нього посадові особи, механізм збору і фіксації доказів, можливі дії по виявленню винуватця;

4. Порядок притягнення винних осіб до дисциплінарної відповідальності;

5. Заходи посилення безпеки, які повинні бути застосовані за підсумками розслідування інциденту;

6. Порядок мінімізації шкоди та усунення наслідків інцидентів.

При розробці регламентів, які опосередковують систему управління подіями ІБ, бажано спиратися на вже створені і показали свою ефективність методики і документи, включаючи форми звітів, журнали реєстрації, повідомлення про подію.

2.3 Досвід організації управління інцидентами в системі забезпечення інформаційної безпеки

Діяльність з інформаційної безпеки здійснюється за допомогою різних методів, прийомів та прийомів, які за своєю органічною сукупністю складають методи. Метод передбачає певну послідовність дій на основі конкретного плану. Методи можуть сильно відрізнятися і змінюватися в залежності від виду діяльності, в якій вони використовуються, та сфери застосування.

Важливими методами аналізу стану інформаційної безпеки є методи опису та класифікації. Для ефективного захисту державного управління спочатку необхідно описати, а потім класифікувати різні типи загроз та небезпек, ризиків та проблем та сформувати систему заходів щодо їх відповідного управління.

Методи дослідження причинності використовуються як загальні методи аналізу інформаційної безпеки. Ці методи виявляють причинність між загрозами, ризиками, викликами та загрозами; шукати причини, що спричинили та спричинили оновлення певних факторів ризику, та вживаються заходи щодо їх усунення. Серед цих методів причинного зв'язку - метод подібності, метод різниці, метод поєднання подібності та відмінностей, метод супутніх змін, метод залишків.

Вибір методів аналізу стану інформаційної безпеки залежить від конкретного рівня та сфери організації безпеки. Залежно від загрози можна виділити різні рівні загроз та різний рівень захисту. Що стосується сфери інформаційної безпеки, то її зазвичай виділяють: фізичну, програмну, управлінську, технологічну, користувацький рівень, мережеву, процедурну. Давайте докладніше розглянемо кожен із цих рівнів.

На фізичному рівні здійснюється організація та фізичний захист інформаційних ресурсів, використаних інформаційних технологій та технологій управління. На програмно-технічному рівні користувачі ідентифікують та засвідчують автентифікацію, контроль доступу, ведення журналів та аудиту, криптографія, скринінг, висока доступність.

На рівні управління координація, контроль та контроль організаційних, технологічних та технічних заходів на всіх рівнях управління здійснюється єдиною системою забезпечення інформаційної безпеки державного управління. На технологічному рівні політика захисту інформації реалізується за допомогою використання комплексу сучасних автоматизованих інформаційних технологій. На рівні користувачів реалізація політики інформаційної безпеки спрямована на зменшення відображаючого впливу на державне управління, унеможливлення впливу на інформаційне середовище соціального середовища. На рівні мережі ця політика реалізується у форматі координації дій органів державної влади, які пов'язані з однією метою. На процесуальному рівні люди вживають заходів. Серед них такі групи процедурних заходів: управління персоналом, фізичний захист, підтримка працездатності, реагування на порушення безпеки, планування реанімації.

Існує кілька типів методів захисту інформації:

• однорівневі методи базуються на одному принципі управління інформаційною безпекою;

• багаторівневі методи базуються на кількох принципах управління інформаційною безпекою, кожен з яких служить для вирішення власної проблеми. Однак приватні технології не пов'язані між собою і орієнтовані лише на конкретні фактори інформаційних загроз;

• складні методи - багаторівневі технології, що інтегруються в єдину систему, координуючи функції організаційного рівня для забезпечення інформаційної безпеки шляхом аналізу набору факторів ризику, які мають сенс або генеруються з єдиного інформаційного центру;

• Інтегровані високоінтелектуальні методи - багаторівневі багатокомпонентні технології, побудовані на потужних автоматизованих, інтелектуальних інструментах управління.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якому етапі управління загрозами. Ці кроки включають: визначення обсягу та контексту інформаційної загрози та складу учасників процесу протидії; прийняття спільної стратегії та схеми дій у політичній, економічній та соціальній сферах життя; забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних підрозділах системи державного управління; Виділення необхідних політичних, економічних, соціальних, адміністративних та організаційних ресурсів, достатніх для реалізації програми для відображення інформаційної загрози та підтримки сталого розвитку суспільних інформаційних ресурсів: перетворення результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю з забезпечення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів із нейтралізації інформаційних загроз. Саме суспільство почасти використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць

в органах державного управління по забезпеченню інформаційної безпеки, не проводиться підготовка відповідних фахівців для органів державного управління.

Вельми важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні індивіда, суспільства і організації заважає розповсюджений міф про те, що захист інформації і криптографія одне й те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпеки лише ототожнюються із захистом інформації шляхом її шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі.

ITIL - библиотека инфраструктуры информационных технологий. Мета процесу Управління Рівнем Сервісу (SLM) не перебуває в простому формуванні SLA(соглашение об уровне предоставления услуги), OLA(договір операційного рівня), каталогу послуг, або ж всього цього разом. Мета процесу - забезпечити зрозумілий замовнику і постачальнику механізм забезпечення підтримки та розвитку інформаційно технологічних(IT)-послуг, моніторингу їх якості. Найбільш ефективно це може бути досягнуто шляхом укладення формальних домовленостей про IT-послуги.

Ключовим елементом процесу є каталог послуг. Каталог послуг це ваш головний інструмент роботи з замовником.

Каталог містить докладний опис діючих послуг на зрозумілій замовнику мовою, а також опис рівнів сервісів, які організація може запропонувати своїм замовникам. В цьому плані каталог є важливим комунікативним інструментом. Каталог послуг може допомогти у формуванні очікувань замовника, споживача (користувача) і тим самим полегшити процес узгодження цілей і завдань замовника і постачальника послуг. Каталог створюється для замовника і тому повинен бути написаний зрозумілою замовнику мовою, а не мовою технічних специфікацій.

Розробляючи каталог послуг, організація (або IT відділ) створює про себе уявлення як про постачальника IT-послуг, а не просто як про технологічну організації, яка виконує впровадження, підтримку або супровід технічних засобів і програмного забезпечення.

CMDB є частиною процесу управління конфігураціями. Концепція CMDB, пропонована ITIL, передбачає створення комплексного всеохоплюючого сховища інформації про IT-середовищі компанії.CMDB [9] це єдиний каталог містить інформацію про всі IT-об'єктах компанії і зв'язках між ними, включаючи:

- Сервера і робочі станції;
- Всі периферійні пристрої та комплектуючі;
- Програмне забезпечення;
- IT-сервіси, а також сервіси одержувані з хмари;
- Мережеве обладнання;
- Принтери, сканери та інше обладнання.

Кожна послуга повинна мати чіткі вимірні параметри. Все, що не можна виміряти (погана якість, хороший рівень, достатня кількість) не повинно бути параметром послуги, тоді як тільки вимірні параметри (з 8.00 до 19.00 у робочі дні; 4 години час усунення збою) повинні включатися в угоди про рівень сервісу.

Сервіс-менеджер: співробітник, який відповідає за надання послуги (послуг). Каталог послуг з самого початку необхідно обговорювати з керівництвом, IT директором, в іншому випадку ви отримаєте каталог послуг IT фахівців, або гірше того, каталог послуг користувачів.

Від споживача послуг бере участь його керівництво, ключові користувачі. У сервісному підрозділі при обговоренні каталогу беруть участь менеджери ресурсних відділів: мережевої інфраструктури, IT інфраструктури, обслуговування IT систем.

Створення каталогу послуг в перший раз - справа не проста. Каталоги послуг бувають в бізнестермінах (бізнес-частина, покупець - бізнес), і в IT термінах (IT частина, покупець послуг - IT підрозділ).

Приклад: Бізнесу потрібна електронна пошта. Для її забезпечення IT закуповує послуги в IT термінах: - обслуговування поштового сервера, обслуговування «заліза», канал зв'язку і ін., то, про ніж бізнес-споживачі послуги знати не зобов'язані.

Вкрай бажано надавати керівництву послуги IT (зовнішні, або IT підрозділу) в бізнес-термінах. Керівники повинні розуміти всі слова і терміни, все не ясне їм необхідно віднести «всередину» послуги, в технічні специфікації, цікаві лише фахівцям. Как именно выбрать услуги.

1. Виділіть послуги, що надаються за запитами: переїзди, обслуговування виїзних нарад. Не вмикайте в каталог проектні послуги: для них інша модель надання (проект має обмежений обсяг, час і бюджет).

2. Складіть реєстр всіх ваших послуг. Послуги повинні бути читані і зрозумілі керівництву. Типові вимоги до каталогу послуг:

• Зрозумілість покупцеві послуги (внутрішнього покупцеві).

• Можливість надання (реалістичність), зрозумілість постачальнику.

• Неподільність послуг (для надання послуги не потрібні інші послуги).

Приклад каталогу послуг:

Реєстр послуг

- А. Базові сервіси
  - про А.1. Обслуговування робочих місць
  - про А.2 Надання електронної пошти
  - про Доступ в Інтернет
  - про Послуга друку
- Послуги зв'язку
  - про Телефонний зв'язок про
  - відеоконференцзв'язок
- Спеціалізовані сервіси
  - про Забезпечення роботи 1С: Бухгалтерія
  - про Забезпечення роботи 1С: Зарплата і кадри
  - про Забезпечення роботи системи «Бюджет»

- Разовые услуги
  - Обеспечение переездов
  - Обеспечение выездных мероприятий

Описание услуг

- А. Базовые сервисы

Услуги общего пользования.

  - А.1. Обслуживание рабочих мест

Параметр	“Золотий рівень”	“Срібний рівень”	“Бронзовий рівень”
Час надання	З 9-00 до 20-00	З 9-00 до 19-00	З 9-00 до 18-30
Допустимий нормативний простій, годин в місяць	1	4	16
Час усунення невиправностей, годин	0,5	2	8
Число консультацій (в зверненнях в місяць)	10	5	1
Консультації надаються по запиту, не пізніше, ніж (годин)	0,5	3	8

Рис. 2.2 Таблиця рівні сервісу

Однією з основних ідей, описаних в ITIL, є ідея організації Service Desk (Диспетчерською служби). Аналіз деяких переваг даної геніальної ідеї, деякі з яких, можливо, не відразу видно з першого погляду.

Отже, як визначає ITIL третьої версії роль і завдання Service Desk. Коротко це можна висловити кількома положеннями:

- Service Desk - спеціалізована функціональна одиниця, орієнтована на обробку специфічних сервісних подій, що надходять у формі звернень користувачів або повідомлень систем моніторингу.
- Service Desk - єдина точка контакту (Single Point Of Contact) між постачальником сервісів і користувачами
- Головна мета (primary aim) Service Desk - відновити нормальний рівень сервісу якомога швидше. В даному випадку «відновлення сервісу» розуміється в самому широкому сенсі: це може включати усунення технічного збою, виконання

запиту на обслуговування, в загальному, все, що необхідно для того, щоб задоволений (задоволений) користувач продовжив свою роботу.

Згідно ITIL, співробітники Service Desk, на відміну від технічних фахівців IT, спеціально орієнтовані / заточені саме на спілкування з простими, часто насилу що можуть пояснити, що трапилося і / або часто перебувають в імпульсивному / подавленому стані користувачами. Цікаво відзначити, що колеги, успішно впровадили Service Desk в своїх компаніях, кажуть, що через деякий час користувачі так звикають до роботи через дружньо налаштований Service Desk, що самі дивуються, як вони раніше могли без нього обходитися [12].

Питання про варіанти і обсязі впровадження ITIL розглядається в книзі «Planning to Implement Service Management», не перекладеною поки на українськумову. Там же наводяться ризики можливих варіантів впровадження.

Всі фактори, що впливають на впровадження розділені на технічні («жорсткі») і психологічні («м'які»). Система Ітіль призначена для зменшення ризиків, пов'язаних з «Жорсткими» чинниками. На думку авторів ITIL, саме «м'які» чинники визначають успіх проекту.

Окремо можна виділити ризик, званий в ITIL «прихованим впровадженням», коли керівництво підприємства не в курсі ініціатив IT служби. Це вірний шлях до провалу проекту. Нижче наведено короткий аналіз варіантів впровадження процесів ITIL.[10]

Варіант впровадження	Огляд варіанту
Впровадження одразу усіх процесів	Таке практично ні де не зустрічається на практиці. Варіант важко реалізується, так як потребує занадто багато уваги зі сторони керівництва IT та компанії.
Впровадження декількох процесів: впровадження Service Desk, управління рівнем сервісу, управління інцидентом	Саме цей варіант надає можливість в найкоротші терміни без значних затрат отримати максимальний результат
Впровадження декількох процесів: Управління змінами та конфігураціями	Часто використовуваний варіант. існують великі ризики, що з впровадженням процесу SLM вам доведеться переглядати навіть поняття «Конфігураційна одиниця».
Однопроцесні стратегії	
Управління інцидентами, служба Service Desk	Це найпоширеніший варіант. Ітіль важає, що впровадження будь-яких процесів ITIL без процесу SLM несе великі ризики для організації та IT відділу. ми вкрай не рекомендуємо його сюди через наступні випадки: -
Впровадження інших процесів ITIL (окремо від інших)	Процеси ITIL вкрай пов'язані з роцесами Управління рівнем сервісу, Управління інцидентами. фактично, впровадження інших процесів ITIL без зазначених двох можливо швидше формальне.

Рис. 2.3. Стратегія впровадження [17]

Іншим завданням захисту є забезпечення постійної інформації під час зберігання або передачі, тобто забезпечення її цілісності. Таким чином, конфіденційність інформації, що надається криптографічними методами, не є головною вимогою при проектуванні публічних систем захисту інформації. Виконання процедур шифрування та декодування може уповільнити передачу даних та зменшити доступ, оскільки державний чиновник запобігає доступу до цих даних та інформації своєчасно та швидко через захищений механізм. Ось чому

конфіденційність інформації повинна відповідати доступу до неї. Тому управління інформаційною безпекою має базуватися на принципі доступності та безпеки. Система захисту інформації повинна, в першу чергу, гарантувати наявність та цілісність інформації та її конфіденційність, коли це необхідно.

Також вплив хакерів та їх здатність суттєво впливати на інформаційні системи дещо перебільшено. Здебільшого були зламані ті системи, які мали слабку безпеку. Наприклад, багато компаній в Україні, які мають солідний грошовий потік і достатні фінансові ресурси, як правило, мають не лише комплексну систему безпеки, але навіть окремо функціонуючу підсистему інформаційної безпеки. Здебільшого інформаційна безпека означає, що доступ до дискети блокується в системних блоках, тим самим запобігаючи несанкціонованому запису інформації. Крім того, системний адміністратор встановлює спеціальні програми фільтрації, які виключають доступ до внутрішньої мережі зовні. Інші методи захисту інформації можна перерахувати, але в той же час ототожнення інформаційної безпеки із захищеністю комп'ютерних систем є лише концептуальною помилкою. Тому не дивно, що більшість українських банків сьогодні втратили чималі гроші внаслідок своєї недбалості. І характерною рисою українського суспільства є те, що жоден з банків ніколи не визнавав факту кібер-злочину, вчиненого проти них.

У цьому аспекті можна відзначити ще одну проблему: нехтування вимогами щодо інформаційної безпеки та відсутність необхідних знань. Здебільшого працівники у своїй роботі відкривають паралельні вікна в Інтернеті і, не усвідомлюючи цього, отримують доступ не лише до інформації, яка зараз обробляється, але загалом до комп’ютерної мережі всієї системи державного управління. , від Кабінету Міністрів України до місцевих органів виконавчої влади, тому одним із найкращих засобів захисту інформації від нападу є запобігання її.

Однак надії не слід давати створенню абсолютної системи захисту інформації, оскільки, як зазначалося вище, у позиції, що загроза та небезпека є складовими системи захисту інформації, тому їх існування та впровадження, а також негативні наслідки, є природним компонентом системи захисту інформації. Вони дають можливість побачити недоліки в системі управління інформаційною безпекою і водночас служать поштовхом до вдосконалення, тобто для розвитку. Тому важливим методом забезпечення інформаційної безпеки є метод розробки.

Захист інформації не обмежується технічними методами, як зазначили багато дослідників. Для ефективної інформаційної безпеки важливі різноманітні моделі та

методи оцінки загроз та важливих факторів. їх мінливість занадто лабільна і залежить як від рівня розвитку цивілізації, так і від контексту оцінки, наявності вичерпних даних про фактори загрози, алгоритму обчислення ймовірності виникнення та величини негативних наслідків. Наявність конкретних даних з цього питання дозволяє нам точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Основним методом аналізу інформаційного ризику є кількісний та якісний аналіз, факторний аналіз та інші. Метою якісної оцінки ризиків є ранжування інформаційних загроз та небезпек за різними критеріями, що дозволить системі сформувати ефективну систему впливу на них.

Критичний сценарій також є важливим методом забезпечення інформаційної безпеки. Ці сценарії аналізують ситуації, коли уявний противник паралізує систему державного управління і, таким чином, знижує можливість підтримувати державне управління в оптимальних параметрах. У той же час аналіз подій у світі дає всі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинених країн.

Також можна вказати на метод моделювання, який дозволяє проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де одна з відомих корпорацій постійно проводить он-лайн освітні дослідження для моделювання різних форм інформаційних атак під час інформаційної війни. Серед методів забезпечення інформаційної безпеки - метод дихотомії. Вживаються необхідні кроки для протидії загрозам інформаційній безпеці як для впливу на джерело загрози, так і для посилення об'єкта безпеки. Відповідно, є дві змістовні сфери протидії. Одна з них формується сукупністю джерел загроз, а інша - сукупністю заходів щодо забезпечення інформаційної безпеки державного управління.

Вплив на джерело загрози інформаційної безпеки полягає у зміні факторів та умов, які можуть завдати шкоди об’єкту безпеки. Мета захисту - переконати противника, що загрози недоцільні. Що стосується органів державної влади, то джерело загроз може бути спрямоване на зміну міждержавних відносин, зміцнення довіри між державами, створення умов, за яких небезпечні дії на об'єкт безпеки стають несприятливими через виникнення небажаних наслідків або неможливі. Основним предметом у цій справі є інформація, яку має противник у вигляді інформації, знань, оцінок. У свою чергу, на інформацію, що надходить від

супротивника, який створює загрозу, може впливати зміна її здатності завдати шкоди, нейтралізувати, перетворити чи усунути її небезпечні властивості. Вплив на інформаційну інфраструктуру важливий у випадках, коли навколишнє середовище може поширювати небезпечну інформацію.

Методи впливу на інформацію у формі повідомлень також можна поділити на електронні та неелектронні. Електронні методи впливу застосовуються, коли повідомлення записуються на електромагнітні носії, призначені для обробки комп'ютерами. Вони повинні знищувати, спотворювати, копіювати повідомлення, що зберігаються на цих пристроях. Це можна зробити лише за допомогою апаратного та програмного забезпечення. Неелектронні методи по суті однакові, але вони реалізовані без використання комп’ютерів для впливу на повідомлення, захисту їх від інших, особливо паперових, носіїв інформації.

Методи впливу на інформаційну інфраструктуру можна поділити на інформаційні та неінформаційні. Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв’язку, автоматизації управління, систем автоматизованої обробки інформації та, таким чином, на запобігання шкоді об'єктам суспільних відносин, що захищаються.

Загалом слід зазначити, що вибір цілей та методів протидії конкретним загрозам та загрозам інформаційній безпеці є важливою проблемою та невід’ємною частиною діяльності щодо реалізації основних напрямів державної політики інформаційної безпеки. Вирішення цієї проблеми визначає можливі форми відповідної діяльності органів державної влади, що вимагає детального аналізу економічних, соціальних, політичних та інших станів суспільства, держави та людини, можливих наслідків вибору тих чи інших варіантів реалізації цих заходи.

Тепер коли стає зрозумілим і сама система забезпечення інформаційної безпеки і її основні положення та мета слід поєднати усі проаналізовані єлементи та розробити рекомендації щодо вдосконалення процесів огранізації управління інцидентами в системі забезпечення інформаційної безпеки підприємства.

3 ДОСЛІДЖЕННЯ ПРОЦЕСІВ ОРГАНІЗАЦІЇ УПРАВЛІННЯ ІНЦИДЕНТАМИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1 Основні процеси організації управління інцидентами

Внаслідок швидкого розвитку інформаційних технологій з'явилися різні інформаційні продукти, які додають цінності існуючим підприємствам, мають інформаційні ресурси та інфраструктуру для їх передачі та мають важливу інформацію про безпеку (ЗІБ) для важливої інформації. З огляду на проведені наукові дослідження щодо організаційного розширення ІБ (ОЗІБ), організація є актуальною та створює наукові передумови для скорочення практичних завдань у роботі ІБ.

ОЗІБ використовує організацію, яка в основному використовує програмні, технічні, фізичні та інші функції ІБ та регулює функціональні інформаційні системи; перевірити інформаційні ресурси; персональний персонал служби ІБ та власне підприємство загалом; Популярні користувачі цієї системи.

ОЗІБ є найрізноманітнішим компонентом загальної організації організації PRI, в інших можливостях є цілі, які є конфіденційними, цілісними і уникають, несанкціонованої, критичної інформації, і вони неонові.

Організаційне управління використовується шляхом планування, інструментального контролю, координації, використання, контролю довільної рідини, довіреної, довіреної, найчастіше перевіреної, яка необхідна для заявлених результатів.

У загальному розумінні ОЗІБ виконує такі функції: інформація (отримана, упакована та вся наявна інформація, яку можна отримати для досягнення цілісних організацій), міжособистісна (дійсно, існує взаємозв'язок між керівниками, особистими, останніми послугами, замовниками та всі необхідні послуги) для прийняття рішення (вибір оптимальної альтернативи, зменшення конфліктів, небезпечне виникнення проблеми) [16].

Відповідь на обробку під час роботи ОЗІБ може бути запропоновано записати цикл процесів управління та представити у своїх планах «Плануй – Виконуй – Перевіряй - Дій» («Plan-Do-CheckAct») [17] (рис. 3.1).

Рис. 3.1. Етапи ОЗІБ

Класифіковані системи безпеки ІБ у всій блоковій системі поділяються на три групи: основи (доступні: база, структура, діяльність, інструменти), кліки (для тих, що розташовані: об'єкти, захищені ІР, обробляються та канальні послуги, управління системою та контроль етап) (а також важливі критичні ресурси, виробництво загрози та зрив, системні вимоги, необхідні дії, вибір системи та управління ними) [18].

У ситуації з ОЗІБ компанія повинна бути пов'язана з аналітичними компаніями, які мають конкретні будинки, які існують у певній кількості та існують у певний час.

До внутрішніх можливостей належать наступні: цілі та діючі компанії використовують ІБ, його структуру, технології, якими вони користуються, та людей (поведінка людей, членів команди, керівників). Зовнішні фактори зазвичай прив’язані до інших, але основними з них є: існуючі фактори, які безпосередньо присутні (політичні сили, існуючі, позиції споживачів, партнери, конкуренти) та

фактори, що підтримують розвиток (стан економіки, науково-технічний прогрес, відповідальність і міжнародні події чому).

Цікаво відзначити, що західні продукти, що використовуються в рамках ОЗІБ, є частиною загальної системи ЗІБ, яка має бути інтегрована у схему «шість «Р»: планування (Planning) - заходи, необхідні для розробки проекту, створення та стратегії ІБ; політика (Policy) - сукупність організаційних принципів, які виконують певну поведінку всередині організації; ІВ програми (Programs), які спеціально управляються як окремі об'єкти; захищена (Protection) - діяльність з управління продуктивністю, включаючи оцінку та контроль рівнів, промислових підприємств, технологій та інструментів; люди (People) - хтось власним правом захищав людину та її власний персонал, затримуючи службу ІБ; Управління проектами - це поточний та керуючий ресурс, який використовується для проектів, результатів та корекції результатів ЗІБ [16].

На думку експертів [19], організаційні структури використовуваних систем можуть бути представлені у сукупності таких рівнів:

Рівень 1 - управління організацією;

Рівень 2 - одиниця ОІБ;

Рівень 3 - адміністратори дотримуються та застосовують різні продукти;

Рівень 4 - відповідний ОІБ у підрозділі (у технологічних розділах);

Рівень 5 - кінцеві користувачі та фізичні особи [19].

Крім того, інформація про захищену організацію може бути доступна третіми сторонами та третіми особами, як партнерами, так і тими, хто потребує місця для роботи в системі ІБ або несанкціонованої, доступної інформації як на місцевому рівні, так і через повідомлення.

Розглядаємо представлені в наукових роботах ОЗІБ. Завдяки своїй функціональній структурі у використанні таких видів діяльності ОЗІБ: пошук та практична реалізація комплексів довгострокової організації організації ІБ та системи внутрішніх вимог, правил та правил; організація підрозділу (відділу, служби, відділу) ІБ; управління інцидентами; перевіряє стан ІБ в організації [17].

Що стосується сфери діяльності, пов'язаної з ЗІБ, компанії окремо відкладають напрямки ОЗІБ: організація режиму та фактично; робота з носіями конфіденційної інформації; робота з персоналом; організація аналітичної роботи та її; комплексне планування роботи з ОЗІБ [19].

Відповідаючи на виробництво, що працює в середовищі ОЗІБ, підприємство залучає та перевіряє цикл затримки управління (планування, організація, контроль, коригування) і залишається поза сферою ЗІБ (зміна та розширення доступу, сертифікація та ліцензування, управління персоналом) [20]. Детальніше показано на рис. 3.2.

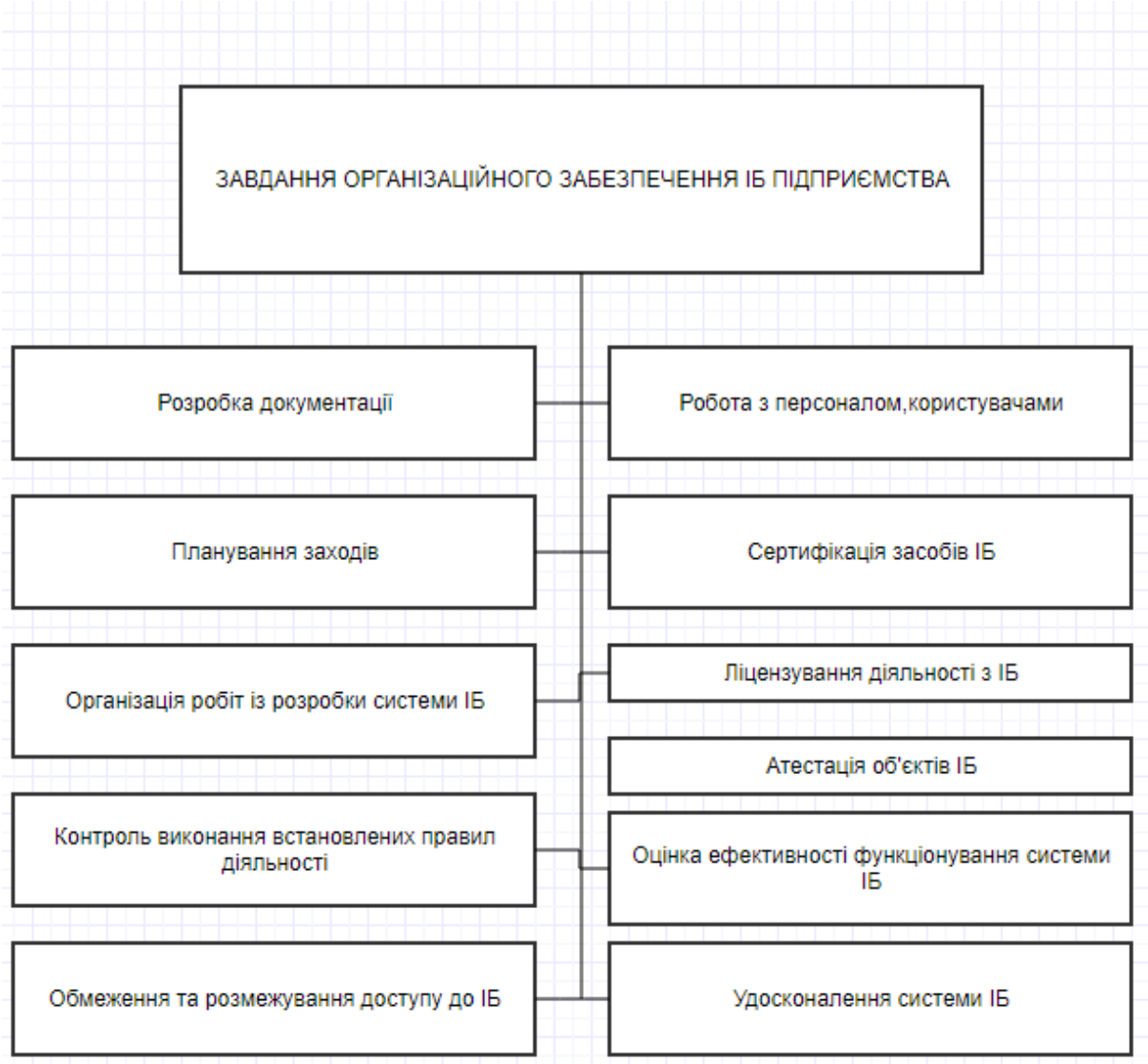

Рис 3.2 Завдання ОЗІБ підприємства.

Узагальнюючи різні наукові підходи [16-22], можна використовувати наступні основні принципи ОЗІБ: складність, доцільно здійснювати тверді повноваження, використовувати, провокувати та методи ЗІБ, щоб зменшити кількість завдань, що залишилися з конкретних питань; адаптованість, яка полягає у адаптації системи ЗІБ до швидко зростаючих підприємств та загрозам;

оперативне прийняття рішень; ефективність, яка допомагає досягти оптимального балансу між іншими продуктами та вживаними продуктами та споживає системи ЗІБ; економічна життєздатність, порівняно з тією, що використовується у ЗІБ, не може нанести великої шкоди при використанні потенційних загроз.

Крім того, ОЗІБ має існуючу систему управління організацією і використовуватиме її у своїх ділових послугах та стратегіях, приєднуючись до провідних галузевих службовців та керівників, використовуючи вказівки, гарантовано дотримуючись необхідних інструкцій та використовуючи Особисті нормы та правила ЗІБ, що ви працюєте на ефективність ЗІБ за допомогою зворотного зв'язку.

Протидія негативним проявам так званого "людського фактора" ОЗІБ приєднується до особистих особистих службовців, які підтримують обов'язки та Міністерство привілеїв; вища освіта та особиста центральність; організація прихильності та уникнення дисциплінарних методів. Успішні умови для успішного ОЗІБ - це створення систем довгого життя, різноманітність функцій безпеки та випуск найсвіжіших посилань [18].

Необхідність своєчасного виявлення інцидентів і реагування на них обумовлена тим, що на карту поставлено не лише конфіденційність, цілісність і доступність інформації, а перш за все репутація та фінанси, яких може позбутися компанія, що не ідентифікувала інцидент, про який сигналізували засоби захисту.
В рамках управління інцидентами ІБ розрізняють два взаємопов'язаних поняття - це подія ІБ і власне сам інцидент ІБ. Подія ІБ - це ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту або раніше невідома ситуація, яка може бути істотною для безпеки.

Подія являє собою логічний зв'язок між дією і об'єктом, на який направлено дана дія, і результатом дії. Іноді виникають події є частиною кроків, що вживаються зловмисником для отримання будь-якого несанкціонованого результату. Ці події можна розглядати як частину інциденту ІБ. Якщо подія виникає знову і може завдати шкоди організації, то така подія потрібно вважати інцидентом ІБ. Інцидент ІБ - це виникнення одного або декількох небажаних або непередбачуваних подій ІБ, в результаті яких велика ймовірність компрометації бізнес-процесів і загрози ІБ для організації.

На сьогоднішній день в організаціях зазвичай виділяють только комп'ютерні інциденті, проти, як ми Вже зумілі переконатися, Поняття інциденту дуже багатогранності. У зв'язку з цим доцільно привести класифікацію інцидентів ІБ:

- комп'ютерні - пов'язані з обробкою інформації в автоматизованих системах;
- технічні - тут мається на увазі вихід / виведення з ладу апаратних засобів;
- організаційні - пов'язані з діяльністю всього персоналу компанії;
- технологічні - процеси виробництва, порушення працездатності технологічних елементів і т.п.

Управління інцидентами - це процес, який відповідає за управління життєвим циклом всіх інцидентів. Основна мета управління інцидентами - це швидке відновлення перерваної роботи для користувачів. Крім того, процес управління інцидентами повинен здійснювати точну реєстрацію всіх інцидентів для оцінки і вдосконалення процесу управління і надання необхідної інформації для інших процесів. Розглянемо етапи процесу управління інцидентами відповідно до ГОСТ ISO / IEC 27001 «Методи і засоби забезпечення безпеки. Системи менеджменту інформаційної безпеки».

1. Планування і підготовка управління інцидентами ІБ [17].

Очевидно, що даний етап є підготовчим і призначений для організації та регламентування діяльності з реагування на інциденти. На даному етапі необхідно:

- забезпечити людські і матеріальні ресурси для відновлення роботи;
- створити схему реагування на інциденти;
- скласти і затвердити ряд організаційно-регламентуючих документів в галузі управління інцидентами;
- ознайомити персонал з нормативними документами, позначити відповідальність за недотримання і провести навчання згідно з розробленою схемою реагування на інциденти;
- провести тестування схеми реагування на інциденти ІБ;
- призначити групу людей відповідальних в розслідуванні і усунення інцидентів;
- скласти перелік можливих інцидентів;
- створити єдину базу даних (БД) всіх виникаючих інцидентів.

2. Використання або експлуатація

Даний етап повинен виконувати функції схеми з реагування на інциденти:

- виявлення інциденту;

- реєстрація інциденту - запис в базу даних і складання звіту, який повинен включати в себе ідентифікатор інциденту, час виявлення, вплив інциденту на бізнес-процес, пріоритет інциденту, ім'я співробітника, який знайшов інцидент і його обов'язки, опис виниклої проблеми, метод зворотного зв'язку;
- оповіщення служби реагування про виникнення інциденту на підприємстві;
- попередній аналіз інциденту (виконується зіставлення виник інциденту з уже трапилися раніше інцидентами, перевіряється наявність можливого рішення або обхідного шляху, також виявляються причини виникнення інциденту);
- оновлення бази даних (пріоритет інциденту, його статус, необхідний час на його усунення, контактні дані групи підтримки, яка прийняла повідомлення про інцидент, дії, здійснені для вирішення інциденту, час і дата його закриття);
- реагування на інцидент (усунення наслідків і причин виникнення інциденту).

3. Аналіз

На даному етапі проводиться поглиблений аналіз інциденту, на основі якого видаються рекомендації щодо поліпшення всього процесу забезпечення інформаційної безпеки і процесу управління інцидентами. Складається звіт, що містить в собі всю інформацію про інцидент.

4. Поліпшення

- реалізація складених рекомендацій щодо поліпшення процесу забезпечення ІБ;
- тестування модернізованої системи.

На перший погляд може здатися, що управління інцидентами вельми складний процес, з точки зору його розробки, так як потрібно виконати безліч дій для його реалізації [19]. У свою чергу, точне проходження даними етапам дозволяє вибудувати ефективний процес, який дозволить в найкоротші терміни вирішити виниклі труднощі і відновити процес роботи (на рис. 3.3).

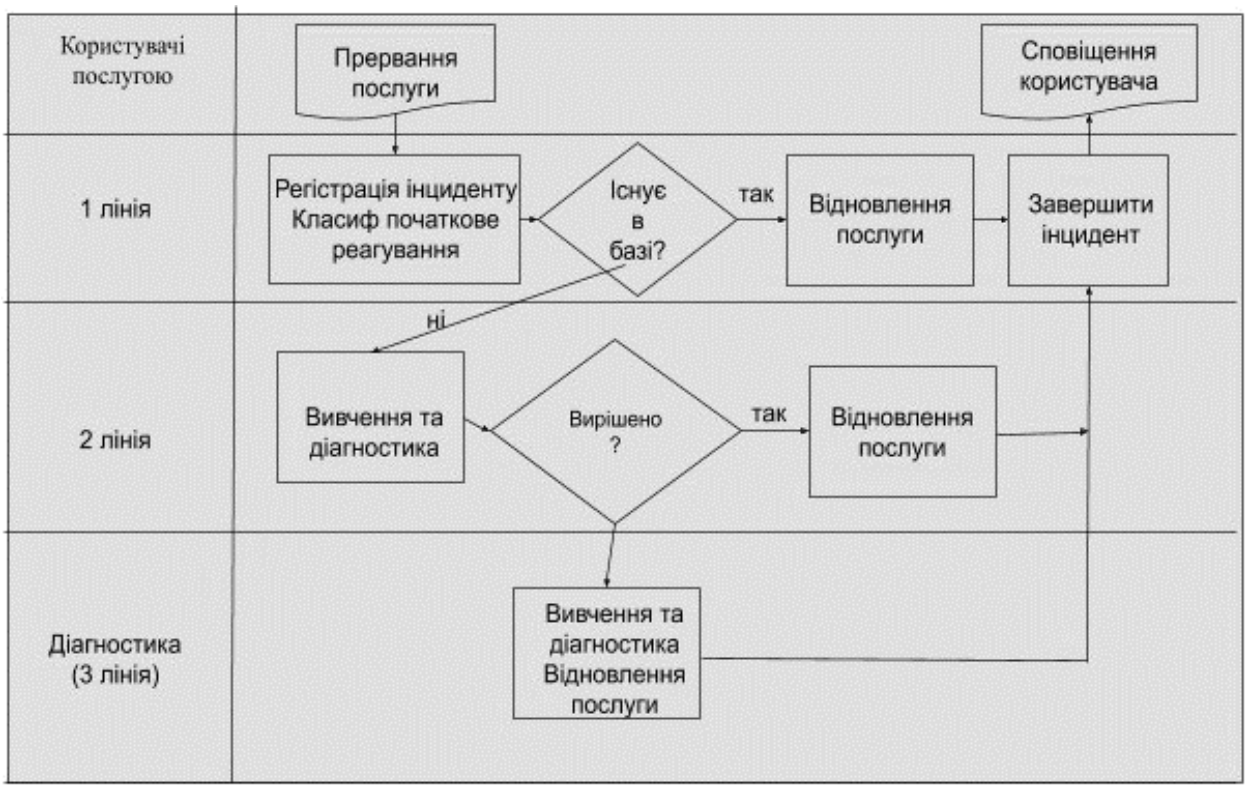

Рис. 3.3 Схема організації управління інцидентами в системі забезпечення

На рис. 3.3 реагування та усунення інцидентів є злагоджена взаємодія процесів, необхідних для ефективного управління інцидентами в компанії. Схема відображає структуру розумної організації системи по управлінню інцидентами ІБ.

Процес управління інцидентами вимагає від персоналу і служби щодо забезпечення інформаційної безпеки чіткої та злагодженої роботи. Не варто забувати про те, що успішне функціонування будь-якого процесу на підприємстві на 90% залежить від персоналу. Тому в обов'язковому порядку потрібно проводити навчання персоналу в області реагування на інциденти, тестувати розроблену схему реагування та відновлення.

Це необхідно для того, щоб жоден виникає інцидент не залишився непоміченим і не перетворився на катастрофу для співробітників організації. Також варто уважно розслідувати і застосовувати заходи щодо усунення для кожного виниклого інциденту за мінімальний період часу. Ефективне управління інцидентами ІБ знижує ймовірність їх повторного виникнення і, як наслідок, мінімізує шкоду, заподіяну ними.

3.2 Інциденти інформаційної безпеки на підприємстві

Закон України «Про основні засади забезпечення кібербезпеки України» використовуючи термін "Інцидент кібербезпеки", визначає його як: подію або сукупність несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, зокрема, пов'язаних з людським фактором) чи таких, що мають ознаки можливої (потенційної) кібератаки, які: становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.[21]

Інциденти ІБ визначають окремі одиниці кризових та надзвичайних ситуацій, які можуть бути приєднані до підприємств інформаційної, соціальної та технічної інфраструктури, які також відокремлені в національних технічних системах - системах та інформаційних матеріалах, що використовуються у державних та державних ресурсах.

Різне розширення під час інцидентів ІБ. Ми завжди бачимо, що існують більш детальні загальнодоступні проблеми, спрямовані на прийняття управлінських рішень у різних ситуаціях (криза).

Щоб побачити управління випадками ІБ, потрібно створити використання цього та ефективного підходу. Це часто найбільш реалістичні та ефективні дії, які можуть бути вжиті та зменшені місією ІБ після звільнення. Для загального управління інцидентами ІБ потрібно залучати до процесу постійного вдосконалення. Це важливо, оскільки так багато нової інформації, і вона не буде ефективною без вдосконалення. [22]

Крім того, існує велика потреба доводити достовірні претензії.

Для початку розроблені відповідні інструкції, які швидко та правильно реагують на інші ІБ. Додавання до цього може підтримувати моніторинг системи, сигналів тощо. Управління ІТ-інцидентами можливо:

1. Процедури для різних випадків ІБ (від ІР та втрати послуг, зловмисного коду, відхилення у випадку, помилок у даних, що не стосуються даних, конфіденційності, зберігання ІР-адреси).

2. Екстрена діагностика (аналіз та виявлення причин інциденту, локалізація, перевірка корисних дій для зменшення рецидиву, відомих з моменту, коли потерпілий отримав тілесні ушкодження або відхилився через те, що він існує, сьогодні можна припустити, що існують огляди послуг та компенсацій програмного забезпечення, доступних лише уповноваженому персоналу).

Управління інцидентами ІБ повинно відповідати керівництву та особистості управління інцидентами ІБ, маючи всі перші пріоритети щодо їх інцидентів.

Інциденти із ІБ можуть трапитися у міжнародних організаціях. Але для цього є потреба реагувати на зростаючу потребу впровадити відповідь та відповідь на інформацію про випадки, які потребують більшість організацій.

Існують також існуючі технології, які дозволяють проводити більше видів моніторингу, існування та використання інцидентів ІБ. Інформація, отримана від інцидентів ІБ, використовувалася для виявлення випадків, які часто повторювались або мали велике значення. Інциденти з інцидентом ІБ можуть вказувати на необхідність додаткового або додаткового контролю для мінімізації пошкодження та зберігання майбутніх інцидентів або можуть бути враховані в конкретному огляді безпеки. Ми завжди можемо оцінити будь-який із варіантів. [23]

У своїй команді вони вважають, що врешті-решт, це проти людини, яка не використовує ІБ після інциденту, яка намагається досягти судової посади, і, таким чином, намагається представити докази. Правила перевірки доказів:

1. Допустимість доказів (Для досягнення результату організація повинна бути впевнена, що її інформаційні системи відповідають будь-яким стандартним або обраним правилам доказів, які можуть бути використані).

2. Варіант доказів (щоб досягти результатів, його слід пропонувати на більш високому рівні доказів і зберігати контролі, які використовуються для правильного та невідмінного, що вказується періодичним зберіганням та виготовленням).

Якщо ІБ розділено, це може бути не зрозумілим, але насправді, що представлено у судових справах. Тому важливо, щоб необхідні докази відповідали навколишньому середовищу або нормальному явищу. У таких випадках організація повинна мати право виступати в якості доказів. Максимізація можливостей для юрисдикційних меж.

3.2.1 Інциденти інформаційної безпеки, пов’язані з роботою персоналу та їх розслідування.

Жоден ідеальний спосіб зменшити ризики інформаційної безпеки, будь то складна політика безпеки чи сучасні брандмауери, не може запобігти появі подій, які потенційно загрожують діяльності організації в інформаційному середовищі. Складність та різноманітність середовища сучасного підприємства призводять до наявності залишкових ризиків незалежно від якості підготовки та проведення заходів протидії. Також завжди існує ймовірність нових, невідомих на сьогодні загроз інформаційній безпеці. Небажання організації займатися подібними ситуаціями може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити понесені збитки [23].

Кількість потенційних витоків досить велика. Найпоширеніші з них - у категорії ненавмисного розголошення працівниками організації з міркувань недостатньої обізнаності або недостатньої дисципліни. Нерозуміння правил поводження з конфіденційними документами, неможливість визначити, які документи є конфіденційними, і звичайна необережність щодо поводження з інформацією може призвести до події або інциденту з інформаційної безпеки.

Ось деякі визначення події та інциденту ІБ:

1. Подія захисту інформації (PIB) означає систему, службу або стан мережі, що вказує на можливе порушення безпеки або невідому ситуацію, яка може бути пов’язана з безпекою, тоді як інцидент захисту інформації (IIB) - це окремий або ряд інформаційної безпеки події, які можуть призвести до збитків для організації. Втрати можуть бути значними (вартість інформації, експлуатаційні витрати тощо) та нематеріальними (репутація організації, мінливий морально-психологічний клімат тощо).

2. Подія захисту інформації - це ідентифікований випадок стану системи чи мережі, який вказує на потенційне порушення політики безпеки інформації або несправності безпеки, або невідому раніше ситуацію, яка може мати значення для політики безпеки. Відповідно, інцидент інформаційної безпеки - це одна подія чи ряд небажаних та непередбачених подій із захисту інформації, які роблять конфіденційною бізнес-інформацію, імовірно, буде оприлюднена [23].

Наприклад, випадки інформаційної безпеки працівників можуть включати:

· Порушення конфіденційності та цілісності цінної інформації;

· Незаконне спостереження за інформаційними системами;
· Знищення інформації;
· Компроміс інформаційної системи (наприклад, розкриття пароля користувача);
· Відмова від послуг, обладнання для обробки інформації, обладнання;
· Пошкодження електромереж;
· Несанкціоноване використання системи для зберігання персональних даних;
· Інші порушення вимог компанії щодо захисту інформації (порушення правил обробки інформації). [24]

Щоб захистити організацію від витоку конфіденційної інформації через її працівників, ви повинні:

· Для контролю доступу працівників до закритих записів та баз даних кожен працівник, незалежно від посади, повинен мати лише ту інформацію, яка їм потрібна для роботи;
· Періодично переглядати дані та визначати ступінь їх конфіденційності;
· Зберігайте важливу інформацію у вогнестійких сейфах із кодовим замком. Необхідно організувати систему класифікації обмеженого доступу різних категорій працівників, які пройшли спеціальне тестування;
· Встановити антивірусне програмне забезпечення на всі ПК та регулярно їх оновлювати;
· Організувати використання копірів працівниками;
· Встановити машину для знищення непотрібних документів (включаючи використаний копіювальний папір);
· Встановити особисту відповідальність працівників за збереження конфіденційної інформації з чіткою мірою дисциплінарного та морального впливу на її витік.

Багато компаній не завжди в змозі відстежувати зміну кількості та характеру МІБ - немає процедури управління інцидентами. Зазвичай відсутність інцидентів не означає, що система управління безпекою працює належним чином, а лише вказує на те, що інцидент не виправлений.

У загальному випадку інцидент ділиться на дві основні категорії, повідомлення про те, що інцидент зараз відбувається, і повідомлення про те, що інцидент може статися найближчим часом.

Одним із кроків, пов'язаних з управлінням інцидентами ІС, є їх розслідування.

Процес розслідування можна розділити на два етапи: збір даних та криміналістичний аналіз.

Аналіз даних включає аналіз файлів журналів роботи, файлів конфігурації, історії Internet Explorer (включаючи файли cookie), електронної пошти та вкладених файлів, встановлених програм, файлів зображень тощо. Необхідно проаналізувати програмне забезпечення, знайти ключові слова, перевірити дату та час інциденту [26].

Криміналістичний аналіз може також включати пошук видалених файлів і областей, втрачені кластери, вільний простір та аналіз відновлених носіїв зі знищених носіїв (наприклад, залишкової намагніченості).

Інформація, зібрана під час першого етапу розслідування, надалі використовується для розробки стратегії реагування на інциденти. Етап аналізу фактично визначає, хто, що, як, коли, де і чому були причетні до інциденту.

Під час розслідування інциденту збирання даних може здійснюватися за допомогою програмного забезпечення, що повторює диск. Це дозволяє зробити резервні копії жорстких дисків автоматизованих робочих станцій користувачів (співробітників компанії) та серверів. Для аналізу даних можуть бути використані спеціальні інструменти для емуляції користувальницьких машин, такі як "VMware Virtual Machine". Аналіз простору на жорсткому диску можна виконати за допомогою спеціалізованого програмного забезпечення "Encase Enterprise Edition" або експертних інструментів Vogon International. Ці два продукти є ключовими у світовому розслідуванні інцидентів ІБ. У деяких випадках для виявлення слідів комп'ютерних інцидентів для "прослуховування" локальної мережі компанії (часто використовують продукт Ettercap - мережевий сніффер) можуть використовуватися різні апаратні та програмні системи.

На етапі розслідування інцидентів важливу роль відіграє реєстрація подій, чіткий розподіл повноважень користувача, відповідальність за вжиті дії - важливі докази особи, яка брала участь у інциденті та які дії він вчинив.

Загальна практика вести нестандартний журнал розслідування інцидентів, розроблений командою реагування.

Ключові позиції таких журналів:

· Поточний стан розслідування;

· Опис інциденту;

· Дії, вжиті командою реагування під час процесу ІІВ;

· Перелік доказів (із обов'язковими джерелами), зібраних у процесі інциденту;
· Коментарі слідчих інцидентів;
· Опис наступного.

Для підвищення ефективності розслідування інцидентів інформаційної безпеки організація повинна мати інженера з інформаційної безпеки, який:
· Розробити політику безпеки (ПБ) з детальними документами, що регулюють діяльність персоналу на всіх рівнях з чітко визначеними обов'язками в межах покладених обов'язків;
· Розробити посадові інструкції, правила, положення з чітко визначеними правами та обов'язками персоналу, пов'язані з поточними бізнес-процесами, які дозволять передбачити наслідки та надійні заходи профілактики для запобігання рецидиву.

Організація повинна розробити відповідний дисциплінарний процес для усунення порушень безпеки та розслідування наслідків інцидентів та вжити відповідних заходів для їх усунення.

Якщо вживати певних заходів для запобігання виникненню інцидентів ІБ, інженера з захисту інформації чи юриста, слід дотримуватися положень чинного законодавства України. Взаємовідносини працівника та роботодавця та відповідальність за порушення інформаційної безпеки організації регулюються Кримінальним кодексом, Адміністративним кодексом та Кодексом законів про працю:

1. За шкоду, заподіяну підприємству, установі, організації при виконанні трудових обов'язків, працівники, з вини яких заподіяна шкода, несуть матеріальну відповідальність у розмірі прямої фактичної втрати, але не більше їх середньої щомісячної збитки сума заробітку. [23]

2. Умисні дії, спрямовані на одержання конфіденційної інформації з метою розголошення або іншим способом використання такої інформації, а також протиправне використання такої інформації, якщо вона заподіяла матеріальну шкоду суб'єкту господарювання, карається штрафом у двісті. до тисячі платників податків. мінімальні доходи, або обмеження волі на строк до п’яти років, або позбавлення волі на строк до трьох років [24].

3. Умисне розголошення торговельної або банківської таємниці без згоди її власника особі, відомій йому у зв’язку з професійною або професійною діяльністю, якщо це робиться з корисливих чи інших особистих мотивів і заподіяло матеріальну шкоду суб’єкту господарювання - карається штрафом. від двохсот до

п'ятисот неоподатковуваних мінімумів доходів громадян, позбавлених права обіймати певні посади або займатися певною діяльністю на строк до трьох років, або виправних робіт на строк до двох років, або позбавлення волі за той самий термін [22].

4. Несанкціоноване перехоплення або копіювання інформації, обробленої на електронних комп’ютерах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинене особою, яка має право на доступ до такої інформації інформація - карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк, а також конфіскувати програмне чи технічне обладнання, яке раніше не здійснювалося для перехоплення або копіювати інформацію, яка є власністю винного [23];

5. Незаконний доступ до інформації, що зберігається, обробляється або передається через автоматизовані системи, тягне за собою штраф від п'яти до десяти неоподатковуваних мінімумів з використанням або без використання засобів, які використовуються для незаконного доступу. [24]

На жаль, компанії часто просто забувають про розслідування інцидентів. Як тільки наслідки інциденту будуть усунені та відновлені бізнес-процеси, не слід вживати подальших дій для розслідування інциденту та вжиття коригуючих заходів.

4. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах(комп’ютерах), автоматизованих системах, комп’ютерних мережах, або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати пев ні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи [23];

5. Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах, - тягне за собою накладання штрафу від п’яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої. [24]

На жаль, про розслідування інцидентів в компаніях часто просто забувають. Як тільки наслідки інциденту усунені, і бізнес-процеси відновлені, подальші дії з розслідування інциденту і здійснення коректуючих заходів не виконуються.

3.2.2 Інциденти інформаційної безпеки, у кібернетичному просторі

Поява перших комп’ютерних мереж забезпечила громадськість засобом швидкого накопичення електронних носіїв всілякої інформації та їх обробки в режимі реального часу. Останні ПКМ різного функціонального призначення, пов'язані між собою програмними, технічними та комунікаційними засобами Інтернету, складають основу інформаційного простору (ІС) сучасного суспільства. Сьогодні Всесвітня павутина (WWW, Web) - це величезний масив інформації про різні людські дії, науку, технології, природу, особистий план тощо. Спеціальне програмне забезпечення для пошуку та переадресації дозволяє користувачам Інтернету одразу отримати необхідну інформацію.

Швидкий розвиток інформаційно-комунікаційних технологій перетворив Інтернет, який має сотні мільярдів документів і охоплює кілька мільярдів користувачів, у світовий депозитарій людських знань. З часом Інтернет захопив соціальні мережі, які наповнили його приватною інформацією та особистими даними та почали впливати на реальне життя суспільства. Інформаційно-комунікаційні технології стали важливою складовою суспільного розвитку, значно змінивши функціонування багатьох державних та державних інститутів. Вони суттєво впливають на формування сучасного інформаційного середовища та дають можливість швидкого накопичення різноманітної тематичної інформації, призначеної для використання в системах аналізу та прийняття рішень.

Кіберпростір - це віртуальне середовище спілкування, створене системою зв’язку між користувачами та інформаційними об’єктами мереж зв'язку всіх форм власності, яка використовується для забезпечення інформаційних потреб суспільства [23].

Завдяки зближенню інформаційно-комунікаційних технологій громадськість стала надзвичайно вразливою до обміну інформацією та стала надзвичайно вразлива до шкідливих кібернетичних впливів та різних видів загроз як інформаційному простору, так і людській свідомості. Питання кібербезпеки,

тобто захист кіберпростору від загрозливого втручання (інцидентів) у роботу інформаційно-комунікаційних мереж, вийшли на перший план [22].

Інциденти, що ставлять під загрозу конфіденційність, цілісність та доступність комп'ютерних даних та систем, відповідно до запропонованої Конвенції Ради Європи про класифікацію кібер-нападів та загроз, поділяються на такі типи [24]:

- несанкціонований доступ до інформаційного середовища (несанкціонований навмисний доступ до комп'ютерної системи або частини її в обхід систем безпеки);
- систематичне втручання (незаконне збурення чи втручання)
функціонування комп'ютерної системи через розробку та розповсюдження вірусного програмного забезпечення, використання апаратних закладок, електронних та інших впливів на апаратні та телекомунікаційні системи);
- перехоплення (незаконний навмисний аудіовізуальний та / або електромагнітний перехоплення)
не обмінюватися комп'ютерними даними, щоб обійти заходи безпеки);
- незаконне використання або повне вилучення комп’ютерного та телекомунікаційного обладнання.

У цьому випадку бувають внутрішні та зовнішні інциденти. Внутрішній інцидент стосується події, яка є джерелом зловмисника, безпосередньо пов'язаного з інформаційною системою, що постраждала. Зовнішня подія вказує на подію, яка є джерелом зловмисника, не пов'язаного безпосередньо з інформаційною системою. Такі події включають вірусні атаки на програмне та апаратне забезпечення ПКМ, атаки відмови у наданні послуг, перехоплення мережевого трафіку, несанкціонований доступ до конфіденційної інформації, сканування корпоративних мережевих порталів, шахрайство в електронних системах управління документами тощо [22]. Найпоширеніші типи атак:

Відмова в сервісі (Denial of Service, DoS) - це атака, яка робить ресурси ПКМ недоступними для авторизованих користувачів. Виконується за допомогою запуску перевантажень ОС, програм або мережевого обладнання. Найбільш поширені DoS-атаки включають повені TCP SYN, повені, потоки ICMP, ідентифікаційний паводк та племінний потоп.

Розподілений відмова в обслуговуванні (DDoS) - це скоординована DoS-атака з багатьох комп'ютерів. Найпоширеніші DDoS-атаки включають повені TCP SYN, потоки TCP, затоплення SYN, UDP, Smurf та ICMP.

Сніфер пакетів (Sniffer) - це програма, яка використовує мережеву інтерфейсну карту, яка працює випадковим чином і перехоплює всі мережеві пакети.

IP-спуфінг (spoof – обман) - це тип хакерської атаки, який передбачає використання зловмисника, який видає себе за чужу IP-адресу.

Віруси (Virus) - це зловмисні фрагменти, які можуть бути вбудовані в інформаційну систему в тілі файлу, який передається користувачем іншим комп'ютерним файлам, включаючи файли системи та програми та електронну пошту.

Мережеві хробаки (Worms) - це шкідливе програмне забезпечення, яке може відтворювати себе та поширюватися на комп'ютери в мережі без участі користувача. Черв'як збирає інформацію про вузли, їх адреси та інші дані, що цікавлять зловмисника.

Трояни (Trojan horse) - це різноманітні шкідливі програми, які маскуються під корисні програми, але шкодять інформаційній системі: вони руйнують або пошкоджують інформацію на диску, крадуть паролі, спотворюють імена файлів тощо.

Логічні бомби (Logic bombs) - це спеціально розроблені коди, які призводять до того, що певна особливість може призвести до відмови програми, зокрема, до її загальної зупинки.

Спам (Spam) - це тип атаки електронною поштою. Велика кількість повідомлень, що надсилаються зловмисником на електронну адресу, заважають поштовим скринькам, а іноді й поштовим серверам.

Ін’єкції (Exploit tools) - це тип атаки, який вводить шкідливі команди або дані в робочу систему, щоб перешкоджати його роботі, отримати доступ до комп'ютера або даних або дестабілізувати систему в цілому. Прикладом такого типу атаки є ін'єкція SQL, яка використовується зловмисниками для зміни налаштувань запитів баз даних (сховищ).

Бекдор (back door) - це шкідлива програма, яка дозволяє зловмиснику отримати доступ до чутливої інформації, що зберігається на віддаленому комп'ютері. Через бекдор, зловмисник може отримати назву корпоративної мережі та EDRPOU, пароль проксі, ім'я поштового сервера, паролі та електронну адресу клієнта із зараженої локальної мережі.

На думку експертів у галузі IT-технологій, Інтернет став ідеальним середовищем для терористичної діяльності, в якому частота та складність кібератак постійно зростають [23].

Сьогодні поява нових зловмисних програм та широке використання таких атак, як кібер-шантаж, підроблені електронні листи, фішинг, SMS-шахрайство, використання ботнетів для організації атак на приватні сайти. Шпигунські та кібер-розвідувальні програми часто використовуються для крадіжки інформації - типу зловмисного програмного забезпечення, яке таємно встановлюється зловмисником на мережевих комп'ютерах для збору конфіденційної інформації про структуру та принципи мережі, виявлення брандмауера, перехоплення та аналіз даних. Найпоширеніші типи шпигунських програм - сканери портів, шпигунські програми клавіатури та екрану, а також кібер-скаути модему та мережі.

Останнім часом хакери використовують досить багато ботнетів (ботнетів, зомбі-мереж), які можуть включати велику кількість заражених комп'ютерів із встановленим зловмисним програмним забезпеченням. Ботнет знаходиться в режимі сну до отримання команди від зловмисника. Після отримання команди ботнет починає виконувати свої функції, пошкоджуючи ресурси атакованої мережі (розкриття IP-адрес та пароля для доступу до інформаційних ресурсів, поширення спаму, атаки на сервери, щоб спровокувати відмову в обслуговуванні клієнтів тощо). Зловмисник може керувати ботом, підключивши відповідний код до одного з комп'ютерів або через веб-сайти, використовуючи попередньо генеровану URL-адресу та використовуючи мережі p2p. Найчастіше ботнети використовуються для організації DDoS-атак.

В останні роки для кіберрозвідки активно використовуються методи моніторингу з відкритим кодом та відносно відкритого джерела (MVVD) та соціальної інженерії (CI), які, на думку національних та західних експертів, забезпечують інтелект від 30% до 90% [24].

Відкритий і відносно відкритий моніторинг - це процес збору широкого спектру інформації про об'єкт розвідки, що супроводжується його обробкою та підготовкою оперативних дій. Соціальна інженерія - це сукупність заходів, розроблених для отримання доступу зловмисників до конфіденційної інформації, яка зовні впливає на цілі працівників та надалі провокує внутрішній інцидент.

Агенти соціальної інженерії використовують такі інструменти, як фішинг, попередження та побиття, щоб підготувати атаку. Фішинг (фішинг, риболовля) - це

використання зловмисником для підробки електронної пошти та надсилання через соціальні мережі шахрайських повідомлень та різних видів вірусних програм для отримання доступу до конфіденційної інформації. Beat - запускає шкідливе програмне забезпечення електронною поштою, відповідаючи на запит зловмисника.

Претекстинг - це дії, в яких зловмисник довіряє жертві та отримує інформацію, що цікавить жертву, використовуючи Skype або телефон та запам'ятовуючи імена реальних людей. У той же час соціальна інженерія означає використання різних вкладок (пристроїв прослуховування, відео- та аудіоспостереження, перехоплення електромагнітних сигналів та запису різних типів випромінювання тощо), замаскованих під предмети побуту, аксесуари для особистого користування, іграшки та більше.

Призначення процесу управління інцидентами - мінімізувати негативний вплив на бізнес за допомогою якнайшвидшого усунення інцидентів. Вимірювання результативності процесу управління інцидентами найчастіше виконується двома метриками: частка своєчасно вирішених інцидентів і середній час усунення інцидентів (в розбивці по рівню впливу або пріоритету - в залежності від того, як визначається термін усунення інциденту). Скорочення часу реакції - один з найбільш очевидних способів скорочення загального часу рішення інцидентів, а отже його можливо виміряти.

3.2.3 Основні метрики інцидентів інформаційної безпеки

Вимірювання - важливий аспект інформаційної безпеки, з яким рано чи пізно стикаються всі фахівці в цій галузі. Відстеження значень метрик дозволяє вчасно виявляти проблеми і вживати заходів щодо їх усунення. [24]

Основною математичною формулою у вимірюванні інциденту є -

$$K = \frac{1}{N} \cdot \sum \frac{T_i}{T_i + Q_i}$$

де N - кількість призначень інцидентів в задану функціональну групу;
Ti - час рішення і-го інциденту (з моменту початку роботи над ним);
Qi - час очікування інциденту в черзі (з моменту призначення до початку обробки).

1. дана метрика що у формулі нормована в діапазоні [0; 1] і має цільову динаміку на зростання;
2. розрахунок даної метрики краще виконувати не для інциденту цілком, а для окремих призначень інциденту в різні групи (оскільки один інциденту може бути послідовно призначений в кілька груп, і навіть кілька разів в одну і ту ж групу);
3. практичніше всього аналізувати значення цієї метрики саме в розрізі по функціональних групах, щоб виявити ті групи, де час реакції вимагає скорочення (з подальшим пошуком кроків, які таке скорочення можуть забезпечити).Щоб врахувати різний вплив інцидентів, можна вибрати один з двох шляхів[23]:
1. виконувати розрахунок даної метрики в розбивці за рівнями впливу / пріоритетам;
2. привести формулу до зваженого середнього, використовуючи в якості ваги Wi рівень впливу або пріоритет інциденту:

$$K = \sum \frac{W_i T_i}{T_i + Q_i} \Big/ \sum W_i$$

Разом з тим складання каталогу метрик - індивідуальний процес для кожної організації. При правильному підході кожна метрика служить певній меті, що залежить від ситуації, і дозволяє отримати відповіді на конкретні питання. Можна сказати, що якщо організація не знає, які метрики в області ІБ їй необхідні, вона не потребує них, так як ще не готова до проведення вимірювань.[27]

Метрики раціональності. Характеризують кількість помилок, що виникають при виконанні процесу, використання тих чи інших механізмів, передбачених для скорочення трудовитрат і т. Д. Наприклад, для процесу управління змінами це може бути метрика «частка (в%) змін, повернутих на повторне оформлення в результаті перевірки менеджером процесу». Для процесу управління інцидентами це може бути «частка (в%) звернень користувачів, закритих після отримання підтвердження по e-mail». Формулювання даних метрик виконується виходячи з опису процедур процесу. Метрики відповідності. «Частка змін, які пройшли вибіркову перевірку у менеджера процесу при закритті» (якщо відповідний норматив визначено в регламенті процесу), «частка фактично проведених аудитів CMDB від загальної кількості аудитів, передбачених річною програмою аудиту

CMDB», причому формулювання метрик виконується виходячи з опису процедур процесу .

Метрики обсягу робіт по виконанню процесу. «Кількість змін, оброблених за місяць (штуки)» або метрика потоку обробки проблем:

$$(N + C) / (O + C),$$

де C - кількість проблем, закритих за період, O - кількість проблем, відкритих за підсумками періоду, N - кількість проблем, зареєстрованих за період, але не закритих до його закінчення. Дані метрики також формулюються на підставі опису процедур процесу.

Досвід виконання різних проектів по організації процесів управління IT дозволяє сформулювати наступні рекомендації з розробки метрик.

Метрик не повинно бути занадто багато. Про кожну метрику розробник повинен бути в змозі пояснити, кому і коли значення цієї метрики допомагає прийняти те чи інше рішення. Велика кількість метрик в регламенті процесу зазвичай говорить про те, що автор документа списав їх з різних джерел. Разом з тим все метрики все одно не придумати - важливіше навчити менеджера процесу принципам формулювання метрик і їх використання в практиці управління процесом.

Метрики обов'язкові для всіх цілей і всіх завдань процесу. Такі метрики дозволяють судити про результативність процесу, а це дуже важливо для стимулювання виконавців, оцінки економічного ефекту і виконання інших управлінських функцій.

Фахівці R-Vision вирішили поділитися власним списком метрик, який сформувався на основі свого досвіду, а також з практики вимірювання ІБ клієнтами. У список увійшли найбільш часто використовувані метрики, які підходять для широкого кола цілей вимірювання і які не потребують великих зусиль при зборі інформації та розрахунках.[28]

Розділили всі метрики на наступні розділи інформаційної безпеки:

- управління інцидентами,
- управління активами,
- управління ризиками,
- управління уразливими,

- аудит ІБ,
- управління ІБ і робота з користувачами.

Для представлених метрик організаціям слід визначити періодичність вимірювання, допустимий і критичний рівні, які дозволять інтерпретувати одержувані значення, а також цільову динаміку. Залежно від змісту, що вкладається в метрику, її цільова динаміка може бути позитивною (допустиме значення вище критичного) або негативною (допустиме значення нижче критичного).[29]

Але оскільки в даній роботі йдеться про саме конкретно інциденти, то й розглядати будемо тільки інциденти.

Метрики у напрямку Управління інцидентами

1. Частка інцидентів за типами

Ставлення числа інцидентів певного типу, виявлених за період часу, до загальної кількості виявлених за цей час інцидентів.

Цільова динаміка: негативна.

Практична цінність: оперативне виявлення проблемних областей ІБ, що вимагають уваги.

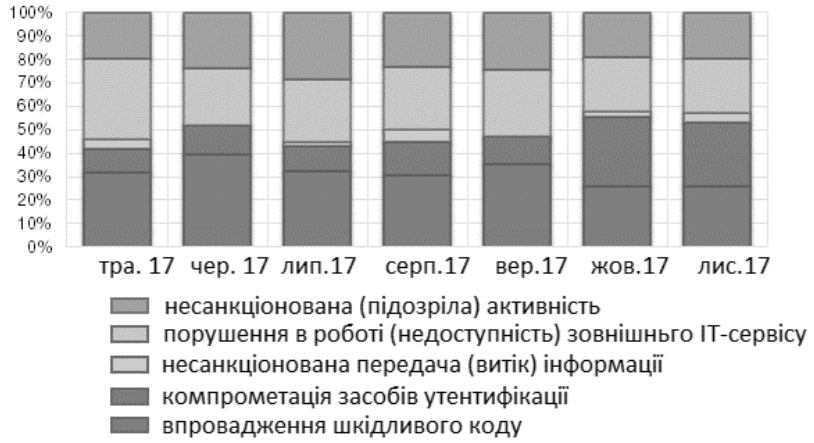

Рис 3.1. Приклад зведення за обраними типами інцидентів

Зростання числа інцидентів певного типу може вказати на виникнення проблеми, що вимагає термінової уваги: відмова в роботі СЗІ, здійснення атаки на організацію і т.д. Відсутність інцидентів деяких типів на певних об'єктах може свідчити про некоректної налаштування SIEM-системи.

Крім того, результати розрахунку даної метрики можуть бути використані при обґрунтуванні керівництву організації необхідності впровадження певного СЗІ [29].

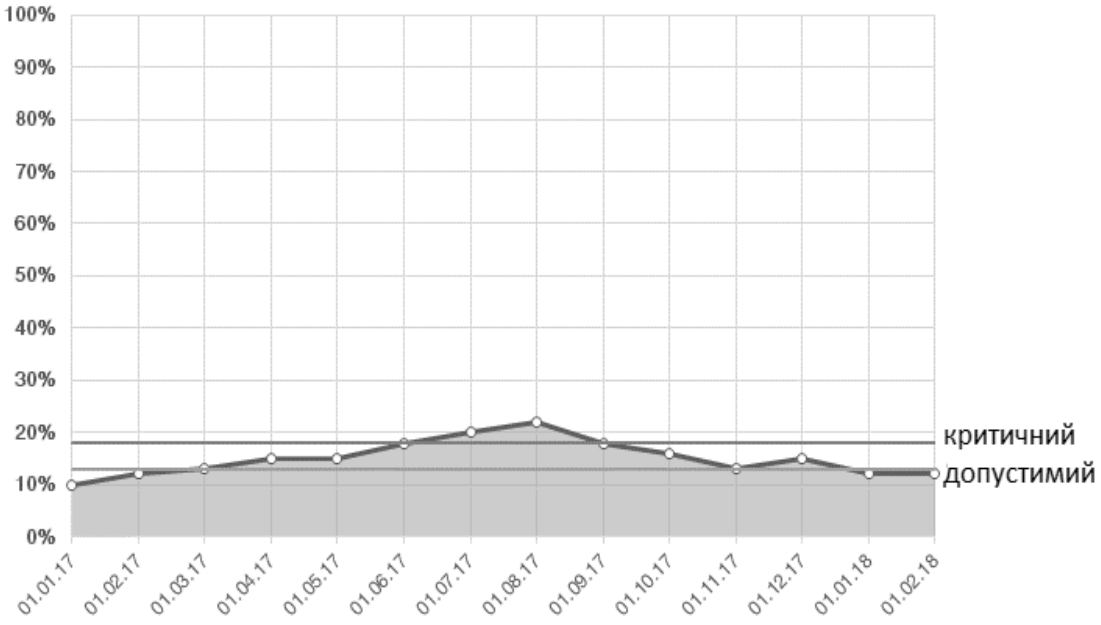

Рис. 3.2. Графік частки інцидентів типу «Впровадження шкідливого коду»

2. Частка інцидентів з дотриманням термінів реагування

Ставлення числа інцидентів, закритих за період часу в встановлені терміни, до загальної кількості закритих за цей час інцидентів.

Цільова динаміка: позитивна.

Практична цінність: оцінка ефективності процесу реагування на інциденти, виявлення проблемних місць [29].

Збільшення цифри не усунених в термін інцидентів може свідчити про надто великий завантаженні групи з реагування на інциденти, порушення в комунікації між її членами, затримках на етапі розслідування інциденту.

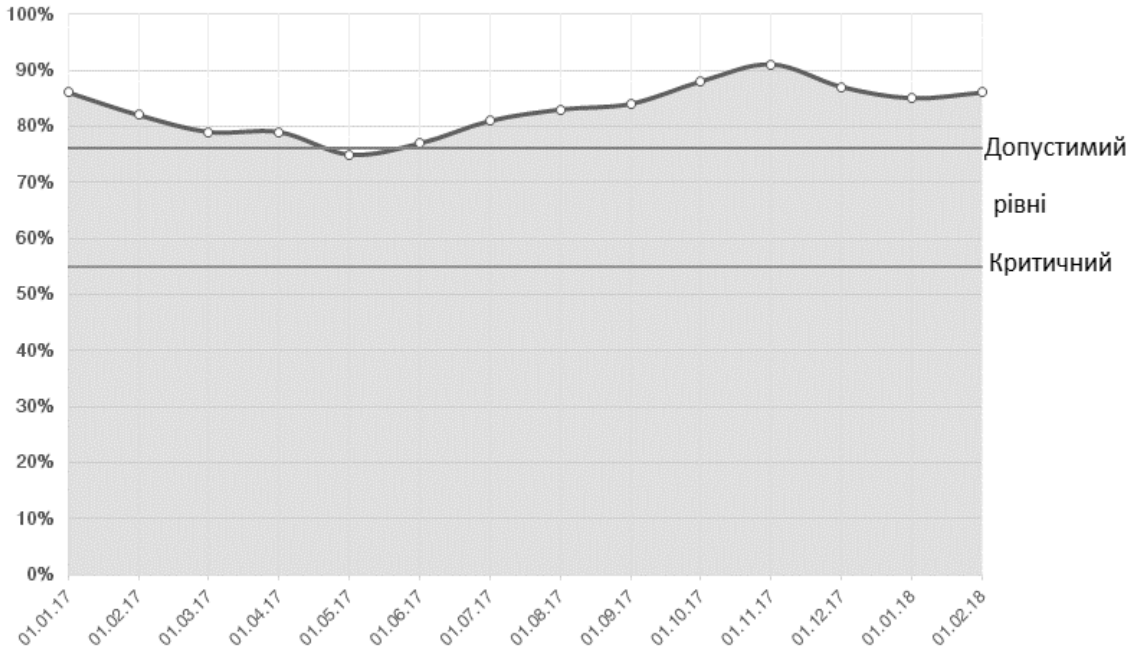

Рис 3.3. Графік частки інцидентів з дотриманням термінів реагування

3. Середній час реагування на інциденти (за рівнями критичності)

Середній час (в годинах), за яке інцидент проходить весь встановлений в організації цикл обробки - від виявлення до закриття. Дану метрику рекомендується розраховувати окремо для кожного рівня критичності.

Цільова динаміка: негативна [29].

Практична цінність: оцінка ефективності процесу реагування на інциденти, визначення шляхів його оптимізації.

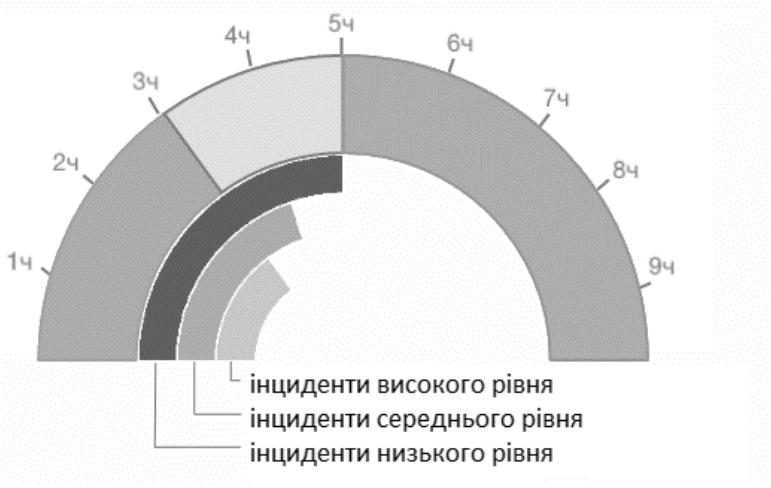

Рис 3.4. Середній час реагування на інциденти (за обраний період)

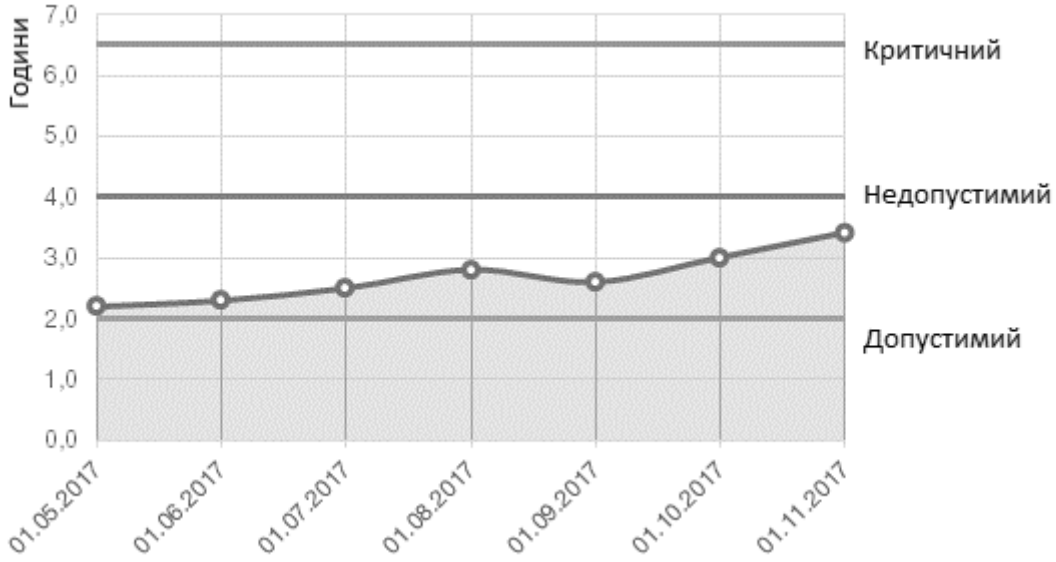

Рис 3.5 Середній час реагування на інциденти високого рівня критичності в динаміці

3.3 Рекомендації щодо вдосконалення процесів організації управління інцидентами в системі забезпечення інформаційної безпеки підприємства (для вибраного прикладу).

Можна створити внутрішньо замкнену систему за високим рівнем контролю та розподілу обовя'зків, завдяки чому більшість інцидентів які є внутрішніми зникнуть, а навіть якщо залишаться то відслідкувати їх буде досить легко.

Від інцидентів які відбуваються по причинам зовнішнім підприємства, не треба нічого нового видумувати коли на даний момент є перевірені методи та способи, програмне забезпечення які допомагають з ними боротись, але все таки деякі рекомендації нижче приведені.

Для успішного впровадження процесів управління інцидентами і проблемами необхідним є дотримання, як мінімум, наступних умов.

Наявність актуальною і своєчасно оновлюваною базою CMDB. Якщо ця база недоступна, інформація про що мають відношення до інциденту одиницях конфігурації буде добуватися вручну, що істотно збільшить час обробки інциденту і підвищить її складність.

Доступність оновлюваної бази знань по помилках / проблемам і способам їх дозволу, а також обходу. Наявність такої бази дозволяє швидко вирішувати багато проблем. Бажано мати можливість підключення до неї аналогічних баз,

розроблених іншими організаціями та компаніями. Виникаючі при цьому питання сумісності можуть привести до великих складнощів, тому рекомендується використовувати рішення з відкритою архітектурою, що містять кошти для імпорту і експорту даних. Останнім часом все частіше в якості стандартного способу доступу до інформації використовується Web-інтерфейс, який є зручним і зрозумілим, а також широко поширеним.

З точки зору потенційно конфліктної ситуації між управлінням проблемами і управлінням інцидентами (через їх різних цілей), необхідно організувати спільну роботу і співпрацю виконавців обох процесів. При цьому не можна забувати про те, що з тих же міркувань один і той же чоловік не може виконувати і ті і інші обов'язки одночасно: йому буде дуже важко знайти баланс інтересів.

Організація ефективної автоматизованої системи реєстрації інцидентів з можливостями детальної і якісної класифікації, що є надзвичайно важливим елементом для організації функціонування як служби Service Desk, так і процесів, що розглядаються в чистому вигляді. Використання для цих цілей паперових технологій не рекомендується.

Організація ефективної автоматизованої системи реєстрації інцидентів з можливостями детальної і якісної класифікації, являВесьма зручно, якщо інструментальні засоби, що використовуються для реалізації розглянутих процесів, мають наступні додатковими можливостями: ющейся надзвичайно важливим елементом для організації функціонування як служби Service Desk, так і процесів, що розглядаються в чистому вигляді . Використання для цих цілей паперових технологій не рекомендується.

- автоматической регистрацией инцидентов, происходящих в наиболее важных устройствах (серверы, сетевое оборудование и т.д.), для чего может потребоваться создание дополнительных интерфейсов;
- автоматической эскалацией инцидентов при нарушении временных графиков;
- гибкой маршрутизацией инцидентов, поскольку персонал служб поддержки может быть размещен в различных помещениях и зданиях;
- автоматическим поиском необходимых данных в базе CMDB;
- специальными решениями для облегчения классификации инцидентов;
- интеграцией с телефонными системами;
- наличием разнообразных диагностических модулей.

Методика підвищення ефективності управління інцидентами підприємтсва. Пропонується використовувати алгоритм управління інцидентами який показує введення додаткової лінії підтримки за рахунок розподілу завдань 1-й лінії, розвантаження обов'язків 2-й лінії. Особливість даної лінії в тому, що вона не вимагає виділення додаткових фахівців, досить задіяти частину фахівців з 1-й лінії, при цьому виявивши мінімальну кількість каналів обробки заявок при заданих обмеженнях. Функції фахівця додаткової лінії технічної підтримки:

- проведення аналізу призначених на робочу групу інцидентів з метою визначення правильності призначення і контролю коректності, зазначених оператором даних;
- розподіл інцидентів по фахівцях 2-й лінії технічної підтримки (інженерам);
- залучення додаткових ресурсів;
- контроль прийняття в роботу і часу виконання інцидентів;
- формування і направлення на регулярній основі фахівцям 2-й лінії підтримки переліку стандартних запитань, які оператор повинен задати, заповнивши контактну форму при прийомі звернення;
- вихідні дзвінки та консультування користувачів по вирішеним заявками;
- консультування з бази прецедентів;
- актуалізація бази знань з письма від фахівців 2-й лінії;
- своєчасне інформування про зміни в системі,

оновленнях або спостережуваних технічних збоях (за листом від фахівців 2-й лінії);

- складання звітності про надходження і направлених заявках, ведення рахунку звернень та інцидентів, оброблених оператором і фахівцями 2-й лінії;
- своєчасне інформування фахівців 2-й лінії про заявках, у яких закінчується термін рішення.

Додаткова лінія підтримки використовує базу прецедентів, де вирішуються питання, які не були вирішені під час розмови з користувачем

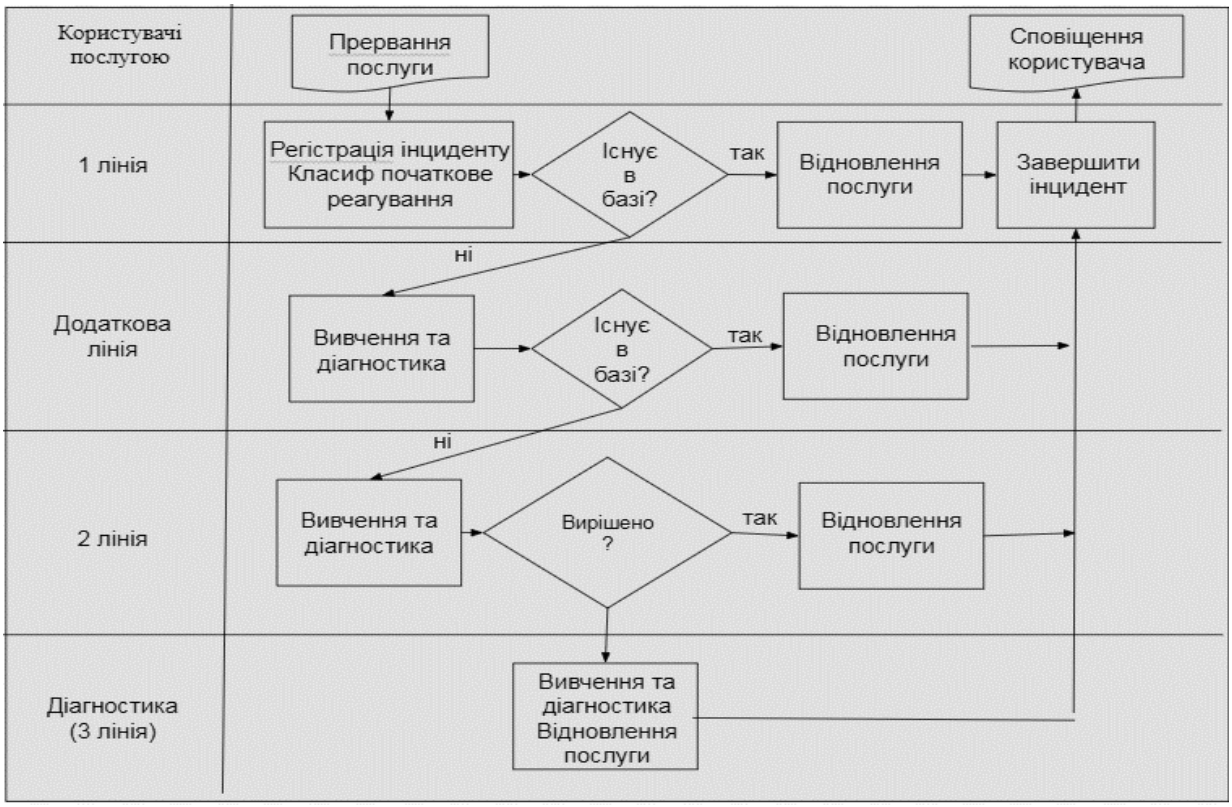

Рис. 3.5. Алгоритм обробки інциденту

Рекомендації щодо організації надійного управління інцидентами.

1. Запропонувати кілька моделей створення заявок, включаючи відправку по електронну пошту, по телефону або через портал самообслуговування.

2. Опублікувати настроюються форми для ефективного збору інформації про IT-інциденти.

3. Налаштувати автоматичну класифікацію та пріоритизації IT-інцидентів на основі критеріїв заявки.

4. Пов'язати SLA з IT-інцидентами на основі таких параметрів заявки, як її пріоритет.

5. Якщо всі технічні фахівці володіють однаковим рівнем знань і навичок, їм можна автоматично призначати заявки на основі таких алгоритмів, як балансування навантаження і циклічний перебір.

6. Пов'язати дані IT-активів, IT-проблеми та IT-зміни з заявками про IT-інциденти.

7. Переконайтися в тому, що закриття інцидентів виконується тільки після надання належного вирішення. Для цього отримаєте підтвердження від кінцевого користувача і застосовуйте відповідні коди закриття.

8. Налаштувати процес комунікації з кінцевим користувачем на кожному з етапів життєвого циклу управління IT-інцидентами.

9. Створити базу знань і постійно поповнюйте її відповідними рішеннями.

10. Забезпечити кінцевим користувачам і технічним фахівцям доступ на основі ролей в залежності від складності рішень.

11. Створити унікальні робочі процеси для обробки серйозних інцидентів.

Важливим аспектом аналізу, який проводять після реагування на інцидент, являється повернення інформації та отриманих знань в схему управління інцидентами інформаційної безпеки. Якщо інцидент інформаційної безпеки достатньо серйозний, то незабаром після вирішення інциденту необхідно провести нараду усіх зацікавлених сторін, володіючих інфомацією про нього. На цій нараді повинні розглядатися наступні питання:

A. Чи належним чином працювали процедури, які було прийнято у схемі управління інформаційною безпекою;

B. Чи існують процедури чи методи, котрі б сприяли виявленню інцидентів;

C. Чи були визначені процедури або засоби, котрі використовувались би у процесі реагування;

D. Чи використовувались процедури, сприяючі відновленню інформаційних систем після ідентифікації інцидента;

E. Чи була ефективна передача інформації усім сторонам учасникам у процесі виявлення, повідомлення та реагування;

Результат наради повинен бути зафіксований у документі (задокументований).

ВИСНОВКИ

Отже провівши аналіз вимог до забезпечення інформаційної безпеки підприємства можна визначити такі основні характеристики інформаційної безпеки підприємства, це дотримання головних принципів: конфіденційність, цілісність, доступність, своєчасність виконуються. Інформаційна безпека підприємництва — це невід’ємна частина інформаційної безпеки України. Інформаційна безпека — це стан захищеності інформаційних ресурсів і потоків, технологічних процесів їх формування і застосування, а також прав суб’єктів інформаційної діяльності. Підприємницька діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків.

Таким чином стає зрозумілим необхідність звернення уваги на інформаційну безпеку в самому підприємстві, тому що ми бачимо на пряму взаємозв`язок цінність інформаційних ресурсів підприємства та розмір витрат у випадках інцидентів. Тому необхідним є приділення уваги інцидентам у сфері системи забезпечення інформаційної безпеки підприємства, для збереження коштів, та сталого розвитку і швидкого реагування на інциденти.

Однак захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємця. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями (властивостями), як корисність, своєчасність і достовірність відомостей які надходять.

Було визначено в процесі дипломної роботи, що забезпечення інформаційної безпеки - це безперервний процес, що включає в себе, п'ять ключових етапів:

- Оцінка вартості
- Розробка політики безпеки
- Реалізація політики
- Кваліфікована підготовка фахівців
- Аудит

Також зрозумілим стає те, що вимоги які несуть у собі стандарти та закони не досконалі, багато прогалин існує, якими можуть скористатись зловмисники, це все також надає переваги впровадження системи забезпечення інформаційної безпеки підприємства, та управління інцидентами в цій системі.

Отже можна сказати, впровадження системи забезпечення інформаційної безпеки, обов’язкова частина успішного підприємства у нинішньому світ, де все йде до великої цінності та боротьби за інформацію. Як було з`ясовано у роботі, забезпечення інформаційної безпеки підприємництва — це низка певних методологій та засобів, направлених на всебічне системне підтримання та вдосконалення рівня захисту інформаційних ресурсів за допомогою виконання відповідними підрозділами системи безпеки завдань щодо:

- розробки організаційних механізмів з технічного захистуінформації від зовнішніх і внутрішніх загроз і для перекриття можливих каналів відтоку інформації в процесі використання засобів зв’язку, передачі та обробки інформації;
- захисту від незаконного проникнення в комп’ютерні системи і мережі, автоматизовані системи;
- захисту інтелектуальної власності та комерційних секретів;
- захисту права суб’єктів господарювання на інформацію;
- захисту інформації шляхом збереження важливої інформації через шифрування невеликих за обсягом відомостей, що містять друковані документи, або перетворення повідомлень, які надсилають за допомогою засобів телефонування.

У результаті розвитку сфери інформаційних технологій та впровадження багатьох програм, інциденти можна рахувати та порівнювати між собою, для покращення швидкості та ефективності реагування на них.

При оцінці процесу покладатися лише на значення метрик можна тільки в тому випадку, якщо дійсно є впевненість, що існуючі метрики дають повну картину, але на практиці так буває не завжди. І причина цього - дорожнеча вимірювання, що робить більш-менш точну оцінку деяких метрик економічно недоцільною.

Також було представлено покращений алгоритм обробки інциденту, завдяки якому додаткова лінія підтримки використовує базу прецедентів, де вирішуються питання, які не були вирішені під час розмови з користувачами.

ПЕРЕЛІК ПОСИЛАННЬ

1. Інформаційна безпека [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki.

2. Галатенко В.А. Интернет Университет Информационных Технологий [Електронний ресурс]. – Режим доступу: http://citforum.ck.ua/security/articles/galatenko.

3. Дудикевич В.Б.,Березюк Б.М.,2017 Особливості інциідентів у сучасному кібернетичному просторі та їх вплив на безпеку суспільства [Електронний ресурс]. – Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/40967/2/2017n880_Dudikevich_V_B-Osoblyvosti_intsydentiv_73-78.pdf.

4. Система забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://pidruchniki.com/12631113/politologiya/sistema_zabezpechennya_informatsiynoyi_bezpeki.

5. Організаційні методи захисту [Електронний ресурс]. – Режим доступу: https://tzi.ua/ua/organzacjn_metodi_zahistu_nformac.html.

6. Комплексна безпека інформаційних мережевих систем [Електронний ресурс]. – Режим доступу: http://kaf-kt.tntu.edu.ua/work/nm/pos/Kompleksna_bezpeka_informatsiynykh_merezhevykh_system.pdf.

7. Управління ризиком [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/управління_ризиком.

8. Что такое CMDB [Електронний ресурс]. – Режим доступу: https://itsm365.ru/blog/articles/chto-takoe-cmdb/.

9. ISO/IEC 27000. Серия стандартов [Електронний ресурс]. – Режим доступу: intercert.com.ua/articles/regulatory-documents/210-iso-27000.

10. Практическая методика внедрения методов ИТИЛ [Електронний ресурс]. – Режим доступу: http://www.adminhelp.pro/wp-content/uploads/2015/05/ITIL-to-10-step.pdf.

11. Стандарти які корисно знати спеціалістам з ІБ [Електронний ресурс]. – Режим доступу: http://80na20.blogspot.com/2013/05/blog-post.html.

12. Service Desk: плюсы явные и скрытые [Електронний ресурс]. – Режим доступу: https://www.itexpert.ru/rus/ITEMS/77-20/.

13. Інформаційна безпека держави: матеріали лекцій. [Електронний ресурс]. – Режим доступу: https://docs.google.com/document/d/1t0Fkjz6H_Po5V_ysXQfc49d8sQaPz2FxRl-Fh9FGOe0/edit.

14. Стандрат ISO/IEC 27035 [Електронний ресурс]. – Режим доступу: https://www.iso27001security.com/html/27035.html.

15. Низенко Е. І. Забезпечення інформаційної безпеки підприємництва / Е. І. Низенко, В. П. Каленяк. – Київ: МАУП, 2006. – 134 с.

16. Інціденти нформаційної безпеки та управління ними [Електронний ресурс]. – Режим доступу: http://wiki.tneu.edu.ua/index.php?title=Інціденти_нформаційної_безпеки_та_управління_ними.

17. Управление инцидентами информационной безопасности [Електронний ресурс]. – Режим доступу: https://studref.com/325292/informatika/upravlenie_intsidentami_informatsionnoy_bezopasnosti#811.

18. Романов О.А. Организационное обеспечение информационной безопасности Учебник для студ. высш.учеб. заведений / О.А. Романов, С.А. Бабин, С.Г. Жданов. - М.: Академия, 2008. - 192 с.

19. Управление информационной безопасностью. [Електронний ресурс]. – Режим доступу: http://www.arinteg.ru/articles/upravlenie-informatsionnoy-bezopasnostyu-26728.html.

20. Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu.

21. Мета функціонування, завдання системи забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://pidruchniki.com/12090613/politologiya/meta_funktsionuvannya_zavdannya_sistemi_zabezpechennya_informatsiynoyi_bezpeki.

22. Мужанова Т. М. Організаційне забезпечення нформаційної безпеки підприємства: основні засади [Електронний ресурс]. – Режим доступу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/693/0.

23. Організація аналітичної роботи [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/15290527/ekonomika/organizatsiya_analitichnoyi_roboti_pidpriyemstvi.

24. Мних Є.В. Економічний аналіз діяльності підприємства : підручник /Є.В. Мних. – К.: Вид-во КНТЕУ, 2008. – 514 с.

25. Ожиганова М.І., Хорошко В.О.,Яремчук Ю.Є.,сКарпінець В.В. Управління персоналом [Електронний ресурс]. – Режим доступу: http://posibnyky.vntu.edu.ua/abooks/petr/Управління_персонаом/p6.html.

26. Інцидент інформаційної безпеки повзязані з роботою персоналу [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/14_ENXXI_2009/Informatica/45935.doc.htm.

27. Виміри процесів. Incident Management. [Електронний ресурс]. – Режим доступу: https://realitsm.ru/2014/01/measuring-incident-management-3/.

28. Організація аналітичної роботи [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/15290527/ekonomika/organizatsiya_analitichnoyi_roboti_pidpriyemstvi.

29. Метрики інцидентів інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://rvision.pro/blog-posts/klyuchevye-metriki-informatsionnoj-bezopasnosti-podborka-ot-r-vision/.

30. Інцидент інформаційної безпеки повзязані з роботою персоналу [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/14_ENXXI_2009/Informatica/45935.doc.htm.

31. Управление информационной безопасностью. [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5199290/.