МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ
ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

«До захисту допущено»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему: **«ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА»**

Студент групи УБДМ-61 Пахомов Валерій Олексійович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

Київ – 2020

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

«Затверджую»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

ЗАВДАННЯ
на магістерську атестаційну роботу
студенту Пахомову Валерію Олексійович

1. Тема роботи: «ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА» затверджена наказом ректора від «___» _____ 20__ р. № __.

2. Термін здачі студентом оформленої роботи: «___» _____ 20__ р.

3. Об’єкт дослідження: інформаційна безпека підприємства.

4. Предмет дослідження: політика інформаційної безпеки підприємства.

5. Мета дослідження: розробка рекомендацій щодо формування політики інформаційної безпеки підприємства.

6. Перелік питань, які мають бути розроблені:
1. Вимоги до формування політики інформаційної безпеки підприємства.
2. Досвід країн у використанні вимог до формування політики інформаційної безпеки підприємств.
3. Рекомендації щодо удосконалення методичних підходів до формування політики інформаційної безпеки підприємства.

7. Дата видачі завдання: «___» _____ 20__ р.

Науковий керівник: Мордас І. В.

Завдання прийнято до виконання: Пахомов В. О.

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської атестаційної роботи
студентом Пахомовим Валерієм Олексійовичем

Дата видачі завдання: «__» _____ 20__ р.

№ з/п	Етапи виконання магістерської атестаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2019	
2.	Збір та аналіз літератури.	18.10.2019	
3.	Написання 1-го розділу роботи.	31.10.2019	
4.	Написання 2-го розділу роботи.	14.11.2019	
5.	Написання 3-го розділу роботи.	28.11.2019	
6.	Формулювання висновків за результатами проведеного дослідження.	05.12.2019	
7.	Оформлення роботи.	12.12.2019	
8.	Оформлення презентації.	19.12.2019	
9.	Отримання рецензії на роботу.	26.12.2019	
10.	Захист в ДЕК.	__.01.2020	

Студент групи УБДМ-61 Пахомов Валерій Олексійович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

РЕФЕРАТ

Робота містить вступ, три розділи з підрозділами, висновки, список використаних джерел та додатки. Загальний обсяг роботи – 90 сторінок.

Об’єкт дослідження – інформаційна безпека підприємства.

Предмет дослідження – політика інформаційної безпеки підприємства.

Мета дослідження – розробка рекомендацій щодо формування політики інформаційної безпеки підприємства.

У магістерській атестаційній роботі проналізовано вимоги до формування політики інформаційної безпеки підприємства; досліджено досвід країн у використанні вимог до формування політики інформаційної безпеки підприємств; розроблено рекомендації щодо удосконалення методичних підходів до формування політики інформаційної безпеки підприємства.

БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ – інформаційна безпека

ПІБ – політика інформаційної безпеки

УІБ – управління інформаційною безпекою

СУІБ – система управління інформаційною безпекою

ВСТУП

Актуальність теми. У міру того, як процес інформатизації більшості областей діяльності нашої країни: уряду, промисловості, соціальної сфери, бізнесу, і т.д. розвивається бурхливими темпами, постає питання про комплексний підхід до захисту інформації. Політика інформаційної безпеки спрямована на вирішення цієї серйозної проблеми. Під політикою інформаційної безпеки розуміють «формальний виклад правил поведінки осіб, які отримують доступ до конфіденційних даних в корпоративній інформаційній системі». Політика, що коректно розроблена і залишається актуальною, відображає думку керіництва з питання інформаційної безпеки, пов'язує воєдино всі методи захисту інформації, дозволяє розробити єдині стандарти в області захисту інформації, регламентує роботу співробітників. Політика інформаційної безпеки є основою для подальшої розробки документів щодо забезпечення безпеки: стандартів, процедур, регламентів, посадових інструкцій і т.д.

Актуальність розробки політики інформаційної безпеки для підприємства пояснюється необхідністю створення механізму управління і планування інформаційної безпеки. Також ПІБ дозволяє удосконалювати наступні напрямки діяльності підприємства:

- підтримка безперервності бізнесу;
- підвищення рівня довіри до підприємства;
- залучення інвестицій;
- мінімізація ризиків бізнесу за допомогою захисту своїх інтересів в інформаційній сфері;
- забезпечення безпечного і адекватного управління підприємством;
- зниження витрат;
- підвищення якості діяльності щодо забезпечення інформаційної безпеки.

Природно, що вдосконалення напрямків діяльності організації залежить від грамотності складання політики інформаційної безпеки. Політика інформаційної безпеки визначає стратегію і тактику побудови системи захисту інформації. Стратегічна частина пов'язана зі стратегією розвитку бізнесу підприємства і розвитком її IT-стратегії. Тактична частина, в свою чергу, детально описує правила безпеки. Відповідно до визначення політики інформаційної безпеки і рекомендаціями міжнародних стандартів в галузі планування та управління ПІБ, політика повинна містити:

- визначення предмета, завдань і цілей;

- умови застосування і їх обмеження;

- відображення позиції керівництва щодо виконання політики ІБ і створення комплексної системи ІБ;

- визначення прав і обов'язків співробітників;

- визначення меж відповідальності співробітників за виконання політики ІБ;

- порядок дій у разі порушення політики ІБ.

Як правило, основна помилка полягає у відсутності на підприємстві формалізованих, зафіксованих і затверджених процесів забезпечення інформаційної безпеки. Ці процеси повинні визначати єдину технічну політику в частині вибору засобів захисту, поточний стан ІБ (рівень зрілості підприємства з точки зору забезпечення інформаційної безпеки) і плани розвитку підприємства.

Мета і завдання дослідження. Мета роботи полягає у розробці рекомендацій щодо формування політики інформаційної безпеки підприємства.

Для досягнення цієї мети в роботі необхідно вирішити такі *завдання*:

1. Проаналізувати вимоги нормативних документів та підходи до розробки політики інформаційної безпеки.

2. Дослідити практику розробки політики інформаційної безпеки в різних країнах.

3. Розробити рекомендації щодо удосконалення методичних підходів до формування політики інформаційної безпеки підприємства.

Об'єктом дослідження є інформаційна безпека підприємства.

Предметом дослідження є політика інформаційної безпеки підприємства.

Методи дослідження. У роботі були використані наступні методи: аналізу та синтезу, порівняння, узагальнення та інші методи.

Практичне значення одержаних результатів. Нові наукові результати, отримані в роботі, складають підґрунтя для розробки універсальної структури політики інформаційної безпеки підприємства.

РОЗДІЛ 1
ВИМОГИ ДО ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Сутність та етапи управління інформаційною безпекою підприємства

Згідно [34], управління інформаційною безпекою - процес, який забезпечує конфіденційність, цілісність і доступність активів, інформації, даних і послуг організації. Управління інформаційною безпекою зазвичай є частиною організаційного підходу до управління безпекою, який має більш широку область охоплення, ніж постачальник послуг, і включає обробку паперових документів, доступ в будівлі, телефонні дзвінки і т.п., для всієї організації.

Основною метою УІБ є забезпечення ефективного управління інформаційною безпекою всіх послуг і діяльностей в рамках управління послуг. Інформаційна безпека призначена для захисту від порушення конфіденційності, доступності та цілісності інформації, інформаційних систем і комунікацій.

Мета забезпечення інформаційної безпеки досягнута, якщо:

1. Інформація доступна тоді, коли це потрібно, а інформаційні системи стійкі до атак, можуть уникати їх або швидко відновлюватися.
2. Інформація доступна тільки тим, хто має відповідні права.
3. Інформація коректна, повна і захищена від неавторизованих змін.
4. Обмін інформацією з партнерами та іншими організаціями надійно захищений.

Щоб забезпечувати інформаційну безпеку і керувати нею, необхідна «система управління інформаційною безпекою». СУІБ - система політик, процесів, стандартів, керівних документів і засобів, які забезпечують організації досягнення цілей управління інформаційною безпекою.

Правильна побудова, впровадження, функціонування, контроль, вчасне коригування, підтримка і поліпшення СУІБ є важливою задачею керівника, який прагне створити конкурентноспроможну, прибуткову, що відповідає законодавству та комерційній репутації, організацію. Для ефективного функціонування СУІБ організації важливим є:

- розуміння вимог, необхідності впровадження політики та цілей інформаційної безпеки;
- впровадження та функціонування важелів контролю з метою управління ризиками інформаційної безпеки;
- контроль і коректування ефективності роботи СУІБ, її безперервне вдосконалення, засноване на об'єктивній оцінці ризиків.

В [37] для організації СУІБ використовуваються наступні етапи: планування, Реалізація, перевірка, дія (табл.1.1).

Таблиця 1.1

Етапи організації СУІБ

Планування (розробка СУІБ)	Розробка політики, встановлення цілей, процесів і процедур СУІБ, що відносяться до управління ризиками і поліпшенню ІБ, для досягнення результатів, відповідних загальній політиці і цілям організації
Реалізація (впровадження та забезпечення функціонування СУІБ)	Впровадження і застосування політики ІБ, заходів управління, процесів і процедур СУІБ
Перевірка (проведення моніторингу та аналізу СУІБ)	Оцінка, в тому числі, кількісна, результативності процесів щодо вимог політики, цілей безпеки та практичного досвіду функціонування СУІБ та інформування вищого керівництва про результати для подальшого аналізу
Дія (підтримка і поліпшення СУІБ)	Проведення коригувальних та попереджувальних дій, заснованих на результатах внутрішнього аудиту або іншої відповідної інформації, та аналізу з боку керівництва в цілях досягнення безперервного поліпшення СУІБ

1.2 Вимоги нормативних документів до формування політики інформаційної безпеки

Останнім часом в різних країнах з'явилося нове покоління стандартів в області інформаційної безпеки, присвячених практичним питанням забезпечення інформаційної безпеки на підприємствах. Це, перш за все, міжнародні стандарти ISO / IEC 17799: 2005 (BS 7799-1: 2002), ISO / IEC 15408, ISO / IEC TR 13335, німецький стандарт BSI IT Protection Manual, стандарти NIST США серії 800, стандарти і бібліотеки CobiT, ITIL, SAC, COSO, SAS 78/94 і деякі інші, аналогічні їм. За цими стандартами політика інформаційної безпеки підприємства повинна визначати наступне [24]:

- предмет політики безпеки, основні цілі і завдання політики безпеки;
- умови застосування політики безпеки і можливі обмеження;
- опис позиції керівництва компанії по відношенню до виконання політики безпеки та організації режиму ІБ компанії в цілому;
- права та обов'язки, а також ступінь відповідальності співробітників за виконання політики безпеки компанії;
- порядок дій в надзвичайних ситуаціях в разі порушення політики безпеки.

В 2013 році вийшла нова версія міжнародного стандарту інформаційної безпеки ISO/IEC 27002:2013. Місце політики інформаційної безпеки у ньому демонструється на рис. 1.1.

На найвищому рівні стандартом вимагається визначити програмний документ – «політика інформаційної безпеки», в якому буде викладено підхід до управління захистом інформації на підприємстві. Цей документ в області інформаційної безпеки повинен бути визначений та затверджений керівництвом, опублікований і доведений до співробітників і відповідних зовнішніх сторін. У [12] програмний документ повинен відповідати таким вимогам:

- бізнес-стратегії;

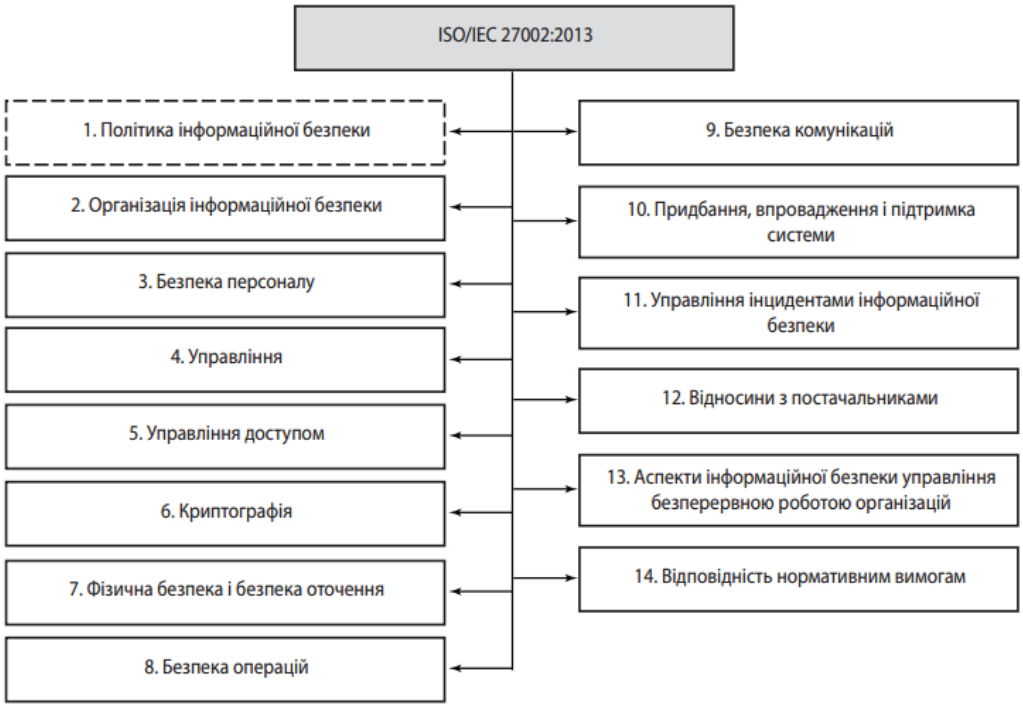

Рис.1.1. Місце політики інформаційної безпеки у міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013

- правилам, законодавству та договорам;
- поточним та прогнозованим загрозам навколишнього середовища щодо інформаційної безпеки.

Політика інформаційної безпеки має містити такі основні відомості:

1. Визначення інформаційної безпеки, її цілей і принципів, що охоплюють всі види діяльності, пов'язані із захистом інформації;
2. Призначення загальних і спеціальних обов'язків з управління інформаційною безпекою;
3. Процесів для обробки відхилень і винятків.

Програмний документ має бути «підтриманий» конкретними темами політики, які сприяють реалізації контролю в області інформаційної безпеки і, як правило, структурований з метою задоволення потреб певних цільових груп усередині організації або для охоплення певних тем, наприклад таких як управління доступом, класифікація інформації (і її обробка), фізична безпека та безпека оточення, конфіденційність і захист персональної інформації та ін.

Політика інформаційної безпеки повинна бути доведена до співробітників і відповідних зовнішніх сторін у формі, яка є доступною і зрозумілою. Крім того, політика інформаційної безпеки може бути оформлена як у вигляді одного документа, так і декількох окремих, але взаємопов'язаних документів; повинна переглядатись через заплановані інтервали або за умови значних змін з метою забезпечення її постійної придатності, адекватності та ефективності.

1.3 Методичні підходи до розробки політики інформаційної безпеки підприємства

Цілями розробки та впровадження політики є:

- визначення основних інформаційних систем і ресурсів, що підлягають захисту;
- формування організаційно-методичної бази для реалізації системи управління інформаційною безпекою.

Основними завданнями, які розв'язуються при розробці політики, є:

- захист інформаційних активів від загроз, що походять від протиправних дій зловмисників;
- управління безперервною роботою системи;
- зменшення ризиків і зниження потенційної шкоди від аварій, ненавмисних помилкових дій персоналу, технічних збоїв, неправильних технологічних і організаційних рішень в процесах обробки, передачі і зберігання інформації, забезпечення нормального функціонування технологічних процесів;
- забезпечення інформаційної безпеки інформаційних ресурсів і систем, а також персоналу організації;
- розробка моделі порушника інформаційної безпеки організації;
- розробка переліку потенційних загроз інформаційній безпеці організації та їх аналіз;

- класифікація інформаційних ресурсів об'єкта та їх контроль;

- формування вимог до СУІБ;

- визначення обов'язків персоналу щодо забезпечення інформаційної безпеки.

Для розробки політики наказом керівника організації затверджується Робоча група, у складі якої обов'язково повинні бути наступні особи:

- представник керівництва організації;

- відповідальний з питань інформаційної безпеки, начальник відділу кадрів (кадрової служби);

- представник технічного персоналу (адміністратор інформаційної безпеки, адміністратор мережі, адміністратор баз даних, або інший компетентний персонал (співробітник)).

При необхідності, можливе залучення інших співробітників організації, сторонніх профільних організацій або фахівців.

При розробці політики ІБ доцільно використовувати модель (рис. 1.2), засновану на адаптації загальних критеріїв і проведенні аналізу ризику [22].

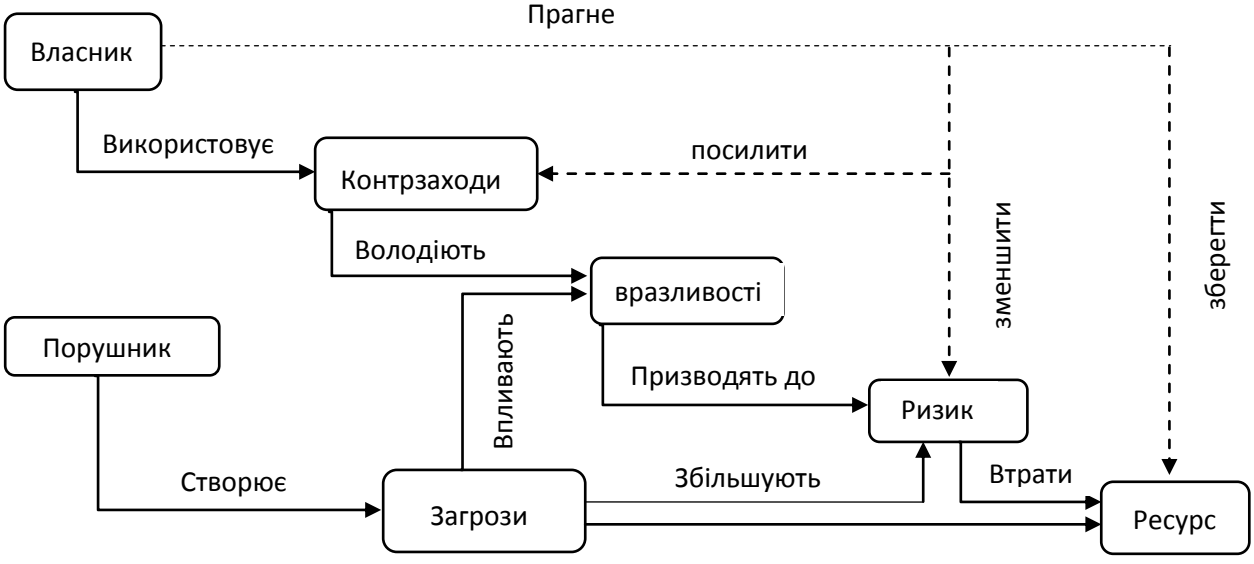

Рис. 2.1. Модель вироблення ПІБ

Ця модель відповідає, міжнародному стандарту ISO / IEC 15408 "Інформаційна технологія - методи захисту - критерії оцінки нформаціонной безпеки", стандарту ISO / IEC 17799 "Управління інформаційною безпекою".

Представлена модель - це сукупність об'єктивних зовнішніх і внутрішніх чинників с урахуванням їх впливу на стан ІБ на об'єкті та на збереження матеріальних або інформаційних ресурсів.

Розглядаються наступні об'єктивні фактори:

- загрози ІБ, що характеризуються вірогідністю виникнення і реалізації;
- вразливість інформаційної системи або системи контрзаходів (підсистеми ІБ), що впливає на ймовірність реалізації загрози;
- ризик, тобто фактор, що відображає можливий збиток підприємства в результаті реалізації загрози ІБ, тобто витоку інформації і її неправомірному використанню (ризик відображає ймовірні фінансові втрати, прямі або непрямі).

Для створення ефективної політики ІБ передбачається спочатку проаналізувати ризики в області ІБ, потім визначити оптимальний рівень ризику для підприємства на основі заданого критерію. Політику ІБ і відповідну підсистему захисту інформації необхідно побудувати так, щоб не перевищити заданого рівня ризику.

Порядок розробки політики розділяється на наступні етапи [23]:

Перший етап - початковий аудит безпеки, в тому числі проведення попереднього обстеження та інвентаризація стану інформаційної безпеки, ідентифікація загроз безпеки підприємства; ідентифікація ресурсів, потребують захисту; визначення ризиків.

В процесі аудиту проводиться аналіз поточного стану ІБ, виявляються існуючі уразливості, найбільш критичні області функціонування і найчутливіші до загроз інформаційній безпеці процеси діяльності підприємства.

Проведення аудиту дозволить визначити загрози і вразливості інформаційної безпеки підприємства, одержати вихідні дані для розробки політики, а також підготувати підприємство до подальшої атестації об'єктів інформатизації.

В ході аудиту організації здійснюється наступне:

- вивчення і аналіз виконання підприємством вимог законодавства України, указів і постанов Президента України і Кабінету Міністрів України, привести у відповідність з категоріями нормативно-правових актів України, а також виконання нормативних документів, що регулюють питання забезпечення інформаційної безпеки на підприємстві;

- первинне обстеження комп'ютерів і серверів підприємства, тобто аналізуються настройки використовуваних операційних систем, прикладного і системного програмного забезпечення, засобів захисту інформації, а також інших апаратних засобів, що входять в інформаційно-комунікаційні технології та ін.;

- аналіз веб-сайту підприємства на предмет наявності загроз і вразливостей інформаційної безпеки;

- аналіз впроваджених заходів забезпечення фізичного захисту території, периметра і приміщень підприємства, тобто аналіз системи охорони, засобів розмежування доступу, системи пожежної безпеки та ін.;

- оцінка обізнаності персоналу підприємства встановленим на підприємстві правилами інформаційної безпеки шляхом інтерв'ювання;

- аналіз категорування і інвентаризації інформаційних та матеріальних ресурсів підприємства.

Другий етап - розробка проекту політики інформаційної безпеки підприємства.

При розробці політики необхідно дотримуватися наступних основних правил:

- політика повинна повністю підкорятися чинному законодавству і вимогам державних стандартів;

- текст політики повинен містити тільки чіткі і однозначні формулювання, що не допускають подвійного тлумачення.

В цілому політика повинна давати чітке уявлення про необхідну поведінку користувачів, адміністраторів та інших фахівців при впровадженні і використанні інформаційних систем і засобів захисту інформації, а також

при здійсненні обміну інформацією і виконання операцій з обробки інформації.

Політика є загальнодоступним документом, який може надаватися без обмежень всім зацікавленим сторонам підприємства.

Третій етап - узгодження і запровадження в дію політики інформаційної безпеки підприємства.

Розроблений проект політики в установленому порядку спрямовується на узгодження до уповноважених органів і після узгодження, вводиться в дію наказом керівника підприємства. При цьому для повноцінного введення в дію затвердженої політики необхідно розробити мережевий план заходів щодо впровадження політики із зазначенням конкретних дат і виконавців.

До посадових інструкцій персоналу, положення про підрозділи, договірні (контрактні) зобов'язання підприємства повинні бути включені обов'язки і відповідальність щодо забезпечення інформаційної безпеки. Необхідно передбачити порядок ознайомлення всього персоналу підприємства до вимог і правил затвердженої політики, а також проведення регулярних роз'яснювальних заходів з питань забезпечення інформаційної безпеки.

Якщо вимоги політики поширюються за межі підприємства, в договірні зобов'язання зі сторонніми підприємствами необхідно включати вимоги інформаційної безпеки.

Перегляд політики необхідно здійснювати не рідше 1 разу на рік, а також в наступних випадках:

- при зміні і затвердження нових нормативно-правових актів і нормативних документів з інформаційної безпеки;
- при зміні конфігурації, додаванні або видаленні програмних і апаратних, програмно-апаратних засобів, що не змінюють технологію інформаційних процесів;
- при зміні конфігурації і налаштувань технічних засобів захисту інформації об'єкта;

- при зміні складу і обов'язків посадових осіб – користувачів і обслуговуючого персоналу об'єкта, що відповідають за її інформаційну безпеку.

Політика підлягає повному перегляду в разі зміни технології інформаційних процесів або використання нових засобів захисту інформації. Проведені заходи щодо інформаційної безпеки підприємства слід регулярно перевіряти на відповідність прийнятій політиці.

Актуалізація і оцінка ефективності політики здійснюється шляхом проведення внутрішнього та зовнішнього аудиту інформаційної інфраструктури підприємства на предмет відповідності вимогам і положенням затвердженої політики.

Регулярність проведення аудиту визначається політикою, при цьому внутрішній аудит повинен проводитися не рідше 1 разу на півроку, а зовнішній аудит не рідше 1 разу на рік.

Висновки до першого розділу

Таким чином, у першому розділі були з’ясовані:

1. Сутність та мета управління інформаційною безпекою.
2. Визначені вимоги нормативнх документів до створення політики інформаційної безпеки.
3. Проаналізовані підходи до створення політики інформаційної безпеки.

Досліджені питання дозволяють проаналізувати досвід різних підприємств щодо розробки ефективної політики інформаційної безпеки.

РОЗДІЛ 2
ДОСВІД КРАЇН У ВИКОРИСТАННІ ВИМОГ ДО ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

2.1 Політики інформаційної безпеки в європейських країнах

В даний час сформувалася так звана краща практика політик інформаційної безпеки. Це перш за все практика розробки політик, процедур, стандартів і керівництв безпеки таких визнаних технологічних лідерів, як IBM, Sun Microsystems, Cisco Systems, Microsoft, Symantec, SANS та ін.

Політика інформаційної безпеки компанії IBM

Фахівці IBM вважають [24], що розробка корпоративних керівних документів в галузі безпеки повинна починатися зі створення політики інформаційної безпеки. При цьому рекомендується використовувати міжнародний стандарт ISO 17799: 2005 та розглядати політику безпеки підприємства як складову частину процесу управління інформаційними ризиками. Вони вважають, що розробка політики інформаційної безпеки відноситься до стратегічних завдань менеджменту підприємства, який здатний адекватно оцінити вартість її інформаційних активів і прийняти обгрунтовані рішення щодо захисту інформації з урахуванням цілей і завдань бізнесу.

Компанія IBM виділяє такі основні етапи розробки політики безпеки:

- визначення інформаційних ризиків підприємства, здатних завдати максимальної шкоди, для розробки в подальшому процедур і заходів щодо попередження їх виникнення;
- розробка політики безпеки, яка описує заходи захисту інформаційних активів, адекватні цілям і задачам бізнесу;

- прийняття планів дій в надзвичайних ситуаціях для зменшення шкоди у випадках, коли обрані заходи захисту не змогли запобігти інциденти в області безпеки;

- оцінка залишкових інформаційних ризиків і прийняття рішення про додаткові інвестиції в засоби і заходи безпеки. Рішення приймає керівництво на основі аналізу залишкових ризиків.

Досвід компанії IBM показав, що політика безпеки підприємства повинна містити явну відповідь на питання «що потрібно захистити?». Таким чином, якщо керівництво підприємства розуміє, що необхідно захистити, які інформаційні ризики і загрози інформаційних активів підприємства існують, тоді можна приступати до створення ефективної політики інформаційної безпеки. При цьому політика безпеки є першим стратегічним документом, який необхідно створити і який містить мінімум технічних деталей, будучи настільки статичним, наскільки можливо.З точки зору IBM, політика безпеки підприємства містить:

- визначення інформаційної безпеки з описом позиції і намірів керівництва підприємства щодо її забезпечення;

- опис вимог з безпеки, в які входить:

- відповідність вимогам законодавства і контрактних зобов'язань;

- навчання з питань інформаційної безпеки;

- попередження і виявлення вірусних атак;

- планування безперервності бізнесу;

- визначення ролей і обов'язків по різним аспектам загальної програми інформаційної безпеки;

- опис вимог і процесу звітності по інцидентах, пов'язаних з інформаційною безпекою;

- опис процесу підтримки політики безпеки.

Для успішної розробки ефективної політики безпеки підприємства фахівцями компанії IBM рекомендується виконати наступні дії:

- аналіз бізнес-стратегії підприємства і визначення вимог щодо інформаційної безпеки;
- аналіз IT-стратегії, поточних проблем інформаційної безпеки та визначення вимог щодо інформаційної безпеки;
- створення політики безпеки, взаємно пов'язаною з бізнес- та IT-стратегіями.

Політика інформаційної безпеки компанії Sun Microsystems

В компанії Sun Microsystems вважають [24], що політика безпеки є необхідною для ефективної організації режиму інформаційної безпеки підприємства. Під політикою безпеки розуміється стратегічний документ, в якому очікування і вимоги керівництва підприємства до організації режиму інформаційної безпеки виражаються в певних вимірних і контрольованих цілях і завданнях.

При цьому Sun рекомендує реалізувати підхід «зверху-вниз», тобто спочатку розробити політику безпеки, а потім приступати до побудови відповідної архітектури корпоративної системи захисту інформації. В іншому випадку політика безпеки буде створена співробітниками служби автоматизації довільно. При цьому архітектура корпоративної системи захисту інформації буде розрізненою, витратною і далеко не оптимальною.

До розробки політики безпеки рекомендується залучити співробітників таких підрозділів підприємства, як:

- керування бізнесом;
- технічне управління;
- відділ захисту інформації;
- департамент управління ризиками;
- департамент системних операцій;
- департамент розробки додатків;
- відділ мережевого адміністрування;

- відділ системного адміністрування;
- служба внутрішнього аудиту та якості;
- юридичний відділ;
- відділ кадрів.

Рекомендована структура документів політики безпеки:

- опис основних цілей і завдань захисту інформації;
- визначення ставлення керівництва підприємства до політики безпеки;
- обгрунтування шляхів реалізації політики безпеки;
- визначення ролей і обов'язків відповідальних за організацію режиму інформаційної безпеки в підприємства;
- визначення необхідних правил і норм безпеки;
- визначення відповідальності за порушення політики;
- визначення порядку перегляду і контролю положень політики безпеки.

Основне призначення політики безпеки - інформування співробітників і керівництва підприємства про існуючі вимоги щодо захисту інформаційних активів компанії. Політика також визначає механізми і способи, які використовуються для досягнення виконання цих вимог. Для цього в політиці безпеки повинні бути визначені показники та критерії захищеності активів підприємства, відповідно до яких будуть купуватися і налаштовуватися засоби захисту. Політика також служить основою для подальшої розробки стандартів, процедур, регламентів безпеки.

Політика безпеки містить очікування керівництва щодо забезпечення безпеки, цілі та завдання організації режиму інформаційної безпеки. Для того щоб бути практичною і здійсненною, політика безпеки повинна реалізовуватися в процедурах, посібниках та стандартах, які забезпечують детальну інтерпретацію положень політики безпеки для співробітників, партнерів і клієнтів підприємства. При цьому рекомендується починати розробку стандартів, процедур і керівництв безпеки після прийняття

політики безпеки і впровадження відповідних механізмів контролю виконання її вимог.

Ключ до успіху політики безпеки - її простота. У зв'язку з тим, що сучасні інформаційні технології, програмне забезпечення та обладнання швидко і постійно удосконалюються і змінюються, політика безпеки повинна бути незалежна від певних програмних і апаратних рішень. На додаток до цього повинні бути явно описані механізми зміни політики безпеки.

Після створення політики безпеки вона повинна бути доведена до відома співробітників підприємства, її партнерів і клієнтів. При цьому бажано доводити політику безпеки через підпис, що підтверджує сам факт ознайомлення з політикою безпеки, а також означає, що всі вимоги політики безпеки зрозумілі і їх зобов'язуються виконувати.

Необхідно організувати процес періодичного перегляду політики, щоб її положення не старіли. В цей процес повинен бути включений механізм внесення змін. Компанія Sun рекомендує створити експертну групу зі співробітників підприємства, які будуть нести відповідальність за регулярний перегляд політики безпеки, перевірку положень політики безпеки на практиці, а також, при необхідності, внесення змін.

Після створення політики безпеки, а також відповідних процедур безпеки ці процедури можуть бути реалізовані в інформаційних системах підприємства. Слід підкреслити, що виконання вимог політики безпеки в системах обробки даних не є достатнім для підтримки довіри клієнтів: не можна гарантувати безпеку без правильної організації обробки даних.

Компанія Sun рекомендує розробляти політику безпеки підприємства на основі кращих практик, описаних у відомих стандартах безпеки, наприклад ISO 17799: 2005. При цьому рекомендується використовувати етапи розробки політики безпеки, зображені в табл. 2.1.

Таблиця 2.1

Етапи розробки політики безпеки компанії Sun

1. Визначення основних цілей і завдань розвитку бізнесу підприємства	Визначення основних цілей і задач розвитку бізнесу підприємства важливо для визначення області застосування політики безпеки. Необхідний відповідний рівень згоди всередині підприємства, що гарантує, що політика безпеки належним чином відображає вимоги безпеки, адекватні цілям і завданням розвитку бізнесу підприємства. Тут важливо розуміти, хто буде визначати політику безпеки підприємства і хто буде займатися її реалізацією і підтримкою. Команда розробників політики безпеки повинна бути представницької і, як мінімум, включати співробітників відділу захисту інформації, юридичного відділу, відділу кадрів, відділу внутрішнього аудиту та якості, відділу системних операцій і відділу програмних розробок
2. Опис основних принципів безпеки	Опис основних принципів забезпечення інформаційної безпеки підприємства дозволяє простим і зрозумілим мовою, не вдаючись у технічні деталі, сформулювати основні цінності підприємства і необхідність їх захисту
3. Класифікація і категорування інформаційних ресурсів	В основі будь-якої політики безпеки лежить визначення цінності інформаційних активів підприємства. Класифікація і категорування інформаційних ресурсів підприємства дозволяє швидко і якісно прийняти рішення про необхідний ступінь захищеності цих ресурсів
4. Аналіз інформаційних потоків	Мета аналізу інформаційних потоків - визначити всі критичні точки обробки даних підприємства. Наприклад, в системі обробки транзакцій дані можуть переміщатися через Web-браузери, сервери даних і міжмережеві екрани і можуть зберігатися в базах даних, на магнітних носіях і на папері. Відстежуючи інформаційні потоки, можна визначити склад і структуру відповідних засобів захисту
5. Визначення основних загроз і моделі порушника	Розробка моделі загроз і моделі порушника дозволяє вирішити, які типи загроз існують в інформаційних системах підприємства, яка ймовірність реалізації загроз і які їхні наслідки, а також вартість відновлення
6. Визначення сервісів безпеки	Визначення сервісів безпеки підприємства, наприклад авторизації, ідентифікації, аутентифікації та ін., дозволяє правильно виробити політику безпеки
7. Створення шаблону політики безпеки	Структура політики безпеки може бути різна. Цей крок використовується для чіткого визначення розділів політики безпеки підприємства
8. Визначення області дії політики безпеки	Останній етап перед створенням перших чорнових варіантів політики безпеки - визначення всіх областей, на яких фокусується політика безпеки

Компанія Sun рекомендує використовувати наступний шаблон політики безпеки:

- розділи: робиться короткий огляд основних розділів політики безпеки;
- заяву про призначення: чому потрібна політика безпеки;
- область дії: яка область дії політики безпеки;
- заяву політики: які специфічні особливості політики безпеки;
- обов'язки: хто і що повинен робити;
- аудиторія: на кого орієнтована політика безпеки;
- впровадження: хто відповідає за впровадження політики безпеки; хто відповідає за порушення політики безпеки;
- виключення: опис можливих винятків;
- інші угоди: опис додаткових угод;
- доведення: хто відповідає за доведення політики безпеки до співробітників; який процес доведення;
- процес перегляду та поновлення: хто відповідає за перегляд і оновлення політики безпеки; що являє собою процес перегляду; з яких причин це відбувається; періодичність перегляду політики безпеки (наприклад, щорічно або при виникненні проблеми);
- здійснення політики: хто відповідає за здійснення політики безпеки; як це виконується;
- моніторинг відповідності: як виконується моніторинг відповідності політики безпеки вимогам бізнесу.

Політика інформаційної безпеки компанії Cisco

З точки зору фахівців Cisco, відсутність ПІБ може призвести до серйозних інцидентів в області безпеки. Розробку політики безпеки підприємства рекомендується починати з оцінки ризиків мережі і створення робочої групи з реагування на інциденти.

Компанія Cisco рекомендує створити політики, які описують ролі і обов'язки співробітників підприємства для належного захисту конфіденційної інформації. При цьому можна почати з розробки головної політики безпеки, в якій чітко прописати спільні цілі і завдання організації режиму інформаційної безпеки підприємства.

ПІБ повинна бути реалістичною і здійсненною, бути короткою і зрозумілою, а також не приводити до істотного зниження загальної продуктивності бізнес підрозділів компанії. Політика безпеки повинна містити основні цілі та завдання організації режиму інформаційної безпеки, чітко містити опис області дії, а також вказувати на контактні особи та їх обов'язки (див. Додаток А). На думку Cisco політика безпеки повинна містити не більше п’яти сторінок тексту, якщо це можливо. При цьому важливо враховувати, як політика безпеки буде впливати на вже існуючі інформаційні системи компанії. Як тільки політика затверджена вона повинна бути надана співробітникам компанії для ознайомлення. Нарешті, політика безпеки повинна переглядатися щорічно, щоб відобразити поточні зміни в розвитку бізнесу компанії.

Наступний крок - створення політики допустимого використання для партнерів, щоб проінформувати партнерів підприємства про те, яка інформація їм доступна. Слід чітко описати будь-які дії, які будуть сприйматися як ворожі, а також можливі способи реагування при виявленні таких дій.

Необхідно створити політику допустимого використання для адміністраторів, щоб описати процедури адміністрування облікових записів співробітників і перевірки привілеїв. При цьому якщо підприємство має певну політику щодо використання паролів або категорування інформації, то потрібно її тут згадати. Далі необхідно перевірити названі політики на несуперечливість і повноту, а також переконатися в тому, що сформульовані вимоги до адміністраторів знайшли своє відображення в планах з навчання.

Потім проводиться аналіз ризиків. Призначення аналізу ризиків полягає в тому, щоб категорувати інформаційні активи підприємства, визначити найбільш значущі загрози і вразливості активів і обґрунтовано вибрати відповідні контрзаходи безпеки. Мається на увазі, що це дозволить знайти і підтримувати прийнятний баланс між безпекою та необхідним рівнем доступу до мережі. Розрізняють такі рівні інформаційних ризиків:

- низький рівень - інформаційні системи і дані, будучи скомпрометованими (доступні для вивчення неавторизованими особами, пошкоджені або загублені), не приведуть до серйозного збитку, фінансовим проблемам або до проблем з правоохоронними органами;
- середній рівень - інформаційні системи і дані, будучи скомпрометованими, приведуть до помірного збитку або до невеликих проблем з правоохоронними органами, або до помірних фінансових проблем, а також до отримання подальшого доступу до інших систем. Порушені системи та інформація вимагають помірних зусиль по відновленню;
- високий рівень - інформаційні системи і дані, будучи скомпрометованими, приведуть до значного збитку або до серйозних проблем з правоохоронними органами, або до фінансових проблем, нанесення шкоди здоров'ю та безпеці співробітників. Системи і інформація вимагають істотних зусиль по відновленню.

Рекомендується визначити рівень ризику для кожного з перерахованих пристроїв: мережеві пристрої, пристрої моніторингу мережі, сервери аутентифікації, поштові сервери, файлові сервери, сервери мережевих додатків, сервери баз даних, персональні комп'ютери та інші пристрої.

При цьому вважається, що мережеве обладнання, таке, як комутатори, маршрутизатори, DNS- і DHCP-сервери в разі компрометації можуть бути використані для подальшого проникнення в мережу і тому повинні ставитися до групи середнього або високого ризику. Можливе пошкодження цих пристроїв може призвести до припинення роботи всієї мережі. Такі інциденти завдають серйозної шкоди підприємству.

Після визначення рівнів ризику необхідно визначити ролі користувачів в цих системах. Фахівці Cisco виділяють п'ять найбільш загальних типів користувачів (табл.2.2).

Таблиця 2.2

Загальні типи користувачів

Адміністратори	Внутрішні користувачі, що відповідають за мережеві ресурси
Привілейовані користувачі	Внутрішні користувачі з необхідністю більшого рівня доступу
Рядові користувачі	Внутрішні користувачі зі звичайним рівнем доступу
Партнери	Зовнішні користувачі з необхідністю доступу до деяких ресурсів
Інші	Зовнішні користувачі або клієнти

Рекомендується створити групу мережевої безпеки під керівництвом менеджера з безпеки з представниками з кожної значущої бізнес-одиниці підприємства (як мінімум з представників бізнес-одиниць розвитку, виконання та виробництва та продажу). Члени групи повинні добре знати політику безпеки та технічні аспекти систем і мереж, що захищаються. Часто це вимагає додаткового навчання співробітників названої групи. Група безпеки повинна брати участь в розробці політики безпеки, організації режиму інформаційної безпеки, а також своєчасно реагувати на інциденти в області інформаційної безпеки компанії.

Процес супроводу політик безпеки полягає в контролі і, при необхідності, перегляд політик безпеки підприємства. Необхідний як мінімум щорічний перегляд політики безпеки і проведення аналізу ризиків.

На практиці група мережевої безпеки повинна проводити аналіз ризиків, підтверджувати запити на проведення змін в системі безпеки, проводити моніторинг повідомлень про появу нових вразливостей з використанням списків розсилок вендорів і незалежних аналітичних центрів,

наприклад CERT або SANS, а також підтримувати відповідність вимогам політики безпеки за допомогою певних технічних і організаційних заходів.

Так як порушення безпеки часто виявляються під час проведення моніторингу мережі, то члени групи мережевої безпеки повинні брати участь в розслідуванні інцидентів та попередження подібних порушень надалі. Кожен член групи безпеки повинен володіти хорошими знаннями в області прикладного, системного і мережевого програмного і апаратного забезпечення систем безпеки. При цьому рекомендується визначити індивідуальні ролі і обов'язки кожного члена групи мережевої безпеки.

Зміни в системах безпеки можуть бути визначені як зміни в мережевому обладнанні, які здатні надати потенційний вплив на стан безпеки мережі. Політика безпеки підприємства повинна визначати специфічні вимоги конфігурації безпеки і містити мінімум технічних деталей. Іншими словами, замість такого визначення вимоги, як «не дозволені зовнішні FTP-з'єднання у внутрішню мережу», потрібно визначити цю вимогу так – «зовнішні з'єднання не повинні бути здатні отримувати файли з внутрішньої мережі». При цьому бажано прагнути до визначення унікальних вимог підприємства. Використання стандартних шаблонів забезпечення безпеки і налаштувань за замовчуванням в підході компанії Cisco не рекомендується.

Група мережевої безпеки переглядає описані загальнодоступною мовою вимоги і визначає відповідність технічного дизайну і налаштувань елементів мережі цим вимогам. Якщо виявляються невідповідності, група безпеки створює необхідні зміни конфігурації мережі для виконання вимог політики безпеки і застосовує їх в подальшому. При цьому групою мережевої безпеки можуть контролюватися не всі зміни. Тут важливо переглянути зміни, найбільш значущі і істотні для мережі підприємства в плані безпеки. Наприклад, до них відносяться зміни:

- в конфігурації міжмережевих екранів;
- в списках контролю доступу;
- в конфігурації SNMP;

- версій програмного забезпечення.

Компанія Cisco рекомендує дотримуватися наступних правил:

- регулярно змінювати паролі на мережевих пристроях;
- обмежити доступ до мережевих пристроїв відповідно до затвердженого списку співробітників;
- гарантувати, що поточна версія програмного забезпечення мережевого і серверного устаткування відповідає вимогам безпеки.

На додаток до цих правил необхідно включити представника групи мережевої безпеки в постійно діючу комісію підприємства за твердженням змін для відстеження всіх змін, що відбуваються в мережі підприємства. Представник групи безпеки може заборонити реалізацію будь-якої зміни, пов'язаного з безпекою, до тих пір, поки ця зміна не буде дозволена керівником групи мережевої безпеки.

Моніторинг мережевої безпеки фокусується на виявленні змін в мережі, що дозволяють визначити порушення безпеки. За відправну точку моніторингу безпеки є визначення поняття «порушення безпеки». Аналіз загроз та інформаційних ризиків дозволяє визначити необхідний рівень повноти моніторингу безпеки мережі підприємства. Надалі при затвердженні змін безпеки кожного разу перевіряється значимість виявлених загроз мережі. Оцінкою цих загроз визначається об'єкт і частота моніторингу.

Рекомендується проводити моніторинг компонент мережі з низьким рівнем ризику - щотижня, із середнім рівнем ризику - щодня, з високим рівнем ризику - раз на годину.

Важливо також визначити в політиці безпеки порядок повідомлення членів групи мережевої безпеки про порушення. Як правило, кошти моніторингу безпеки мережі будуть першими автономно виявляти порушення. Повинна бути передбачена можливість відправки по будь-яким доступним каналам зв'язку повідомлень в центр реагування на інциденти в області безпеки для оперативного оповіщення членів групи мережевої безпеки.

При виявленні порушення безпеки важливо своєчасно відреагувати і оперативно відновити нормальне функціонування сервісів мережі. Тут головне правило - своєчасне оповіщення групи мережевої безпеки після виявлення порушення. Якщо це правило не виконується, то реагування буде загальмовано, а отже, вторгнення і наслідки важчими. Тому необхідно розробити відповідну процедуру реагування та оповіщення, здатну діяти цілодобово.

Далі необхідно чітко визначити рівень привілеїв по внесенню змін, а також порядок внесення змін. Тут можливі наступні коригувальні дії:

- реалізація змін для попередження подальшого поширення порушення;
- ізолювання пошкоджених систем;
- взаємодія з провайдером для відстеження джерела атаки;
- використання записуючих пристроїв для збору доказів;
- відключення пошкоджених систем або джерел атаки;
- звернення до правоохоронних органів або федеральні агентства;
- виключення пошкоджених систем;
- відновлення систем відповідно до списку пріоритетності;
- повідомлення керівництва і юристів компанії.

Необхідно деталізувати будь-які зміни в політиці безпеки, які можуть бути зроблені без обов'язкового отримання дозволу від керівництва.

Відзначено, що існують дві основні причини для збору і зберігання інформації про атаки: визначення наслідків реалізації атаки і розслідування і переслідування зловмисник. Тип інформації, спосіб збору та обробка інформації обумовлені цілями реагування на порушення безпеки.

Для визначення наслідків порушення безпеки рекомендується здійснити наступні кроки:

- зафіксувати інцидент з допомогою записи мережевого трафіку, зняття копій файлів журналів, активних облікових записів і здійснювати підключення до мережі;

- обмежити подальші порушення шляхом відключення облікових записів, від'єднання мережевого обладнання від мережі і від Інтернету;

- провести резервне копіювання скомпрометованих систем для проведення детального аналізу пошкоджень і методу атаки;

- спробувати знайти інші підтвердження компрометації. Часто при компрометації системи виявляються порушеними інші системи і облікові записи;

- переглядати збережені файли журналів пристроїв безпеки і мережевого моніторингу, так як вони часто є ключем для визначення методу атаки.

Якщо необхідно провести юридичні дії, слід повідомити керівництво і залучити юристів підприємства для збору відповідних доказів. Якщо порушення було внутрішнім, то буде потрібно залучити співробітників відділу кадрів підприємства.

Кінцевою метою процедури реагування на порушення в галузі безпеки є відновлення роботи сервісів мережі підприємства. Тут необхідно визначити порядок відновлення доступності сервісів, наприклад за допомогою процедур резервного копіювання. При цьому треба враховувати, що кожна система має свої власні механізми резервного копіювання. Тому політика безпеки, будучи загальною для всіх елементів мережі, при необхідності повинна дозволяти деталізувати умови відновлення конкретного елемента. Якщо потрібно отримати дозвіл на відновлення, потрібно описати порядок отримання дозволу в політиці безпеки.

Перегляд політики безпеки є заключним етапом життєвого циклу політики безпеки. Тут важливо звернути увагу на наступне. Політика безпеки повинна бути «життєздатним» документом, адаптованим до умов, що змінюються. Порівняння існуючої політики безпеки з кращими практиками в цій області і подальший перегляд політики повинні підтримувати в актуальному стані захищеність активів мережі. Необхідно регулярно звертатися на Web-сайти різних незалежних аналітичних центрів, наприклад

CERT або SANS, за корисними порадами та рекомендаціями щодо забезпечення безпеки і враховувати їх в підтримуваної політиці безпеки компанії.

Також рекомендується проводити аудит безпеки мережі шляхом звернення до відповідних консалтингових компаній, що спеціалізуються на наданні подібних послуг. Для мереж з високими вимогами до доступності інформаційних ресурсів рекомендується проведення незалежного аудиту безпеки як мінімум раз на рік. Крім того, досить ефективні і внутрішні тренування для відпрацювання дій в надзвичайних ситуаціях.

Політика інформаційної безпеки компанії SANS

Організація SANS виробила свій підхід в розумінні політики інформаційної безпеки та її складових. У термінології SANS політика інформаційної безпеки - багаторівневий документований план забезпечення інформаційної безпеки підприємства (рис. 2.1):

Рис. 2.1. Структура керівних документів інформаційної безпеки підприємства

- верхній рівень - політики;
- середній рівень - стандарти і керівництва;
- нижчий рівень - процедури.

Далі документи розбиваються на наступні основні категорії:

- твердження керівництва про підтримку політики інформаційної безпеки;
- основні політики підприємства;
- функціональні політики;
- обов'язкові стандарти (базові);
- рекомендовані керівництва;
- деталізовані процедури.

Стандарти деталізують відмінності по налаштуванню безпеки в окремих операційних системах, додатках і базах даних.

Керівництва являють собою рекомендовані, необов'язкові до виконання дії по запобіганню проблемам, пов'язаних з різними аспектами інформаційної безпеки.

Процедури - детальні покрокові інструкції, які співробітники зобов'язані неухильно виконувати.

При розробці політик дуже важливим є коректний розподіл ролей і обов'язків. Дуже важливо дотримуватися принципу найменших привілеїв, принцип «знати тільки те, що необхідно для виконання службових обов'язків» і використовувати поділ обов'язків на критичних системах.

Розрізняють такі типи політик безпеки:

- спрямовані на вирішення конкретної проблеми - прикладами таких політик можуть служити політика по найму персоналу, політика використання паролів, політика використання Інтернету;
- програмні - високорівневі політики, що визначають загальний підхід компанії до забезпечення режиму інформаційної безпеки. Ці політики визначають напрямок розробки інших політик і відповідність до вимог законодавства та галузевих стандартів;
- застосовуються до конкретного середовища - наприклад, кожна операційна система вимагає окремого стандарту з її налаштування.

Рекомендовані компоненти політики безпеки:

- мета;
- область дії;
- твердження політики;
- історія документа;
- необхідність політики;
- які політики скасовує;
- дії по виконанню політики;
- відповідальність;
- виключення;
- порядок і періодичність перегляду.

Організація SANS розробила ряд шаблонів політик безпеки:

- політика допустимого шифрування;
- політика допустимого використання;
- керівництво з антивірусного захисту;
- політика аудиту вразливостей;
- політика зберігання електронної пошти;
- політика використання електронної пошти підприємства;
- політика використання паролів;
- політика оцінки ризиків;
- політика безпеки маршрутизатора;
- політика забезпечення безпеки серверів;
- політика віртуальних приватних мереж;
- політика бездротового доступу в мережу підприємства;
- політика автоматичного перенаправлення електронної пошти підприємства;
- політика класифікації інформації;
- політика щодо паролів для доступу до баз даних;
- політика безпеки лабораторії демілітаризованої зони;
- політика безпеки внутрішньої лабораторії;
- політика екстранет;

- політика етики;
- політика лабораторії антивірусного захисту.

2.2 Політики інформаційної безпеки в Росії

Темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендаційної і нормативно-правової бази керівних документів, що діють на території Росії. Тому вирішення питання про розробку політики інформаційної безпеки на сучасному підприємстві пов'язано з проблемою вибору критеріїв і показників захищеності, а також ефективності корпоративної системи захисту інформації. Внаслідок цього на додаток до вимог і рекомендацій стандартів, Конституції і федеральним законам, з керівними документами Гостехкомісії (ФСТЕК) Росії доводиться використовувати ряд міжнародних рекомендацій. У тому числі адаптувати до вітчизняних умов і застосовувати на практиці відповідно до рекомендацій Федерального закону № 184-ФЗ "Про технічне регулювання" методики міжнародних стандартів, таких, як ISO 17799 (BS 7799), ISO 9001, ISO 15408, ISO 13335, BSI, CobiT, ITIL та ін., а також використовувати методики управління інформаційними ризиками в сукупності з оцінками економічної ефективності інвестицій в забезпечення захисту інформації підприємства.

Сучасні методики управління ризиками дозволяють в рамках політик безпеки російських підприємств поставити і вирішити ряд завдань перспективного стратегічного розвитку.

По-перше, кількісно оцінити поточний рівень інформаційної безпеки підприємства, що потребують виявлення ризиків на правовому, організаційно-управлінському, технологічному, а також технічному рівнях забезпечення захисту інформації.

По-друге, розробити політику безпеки і плани вдосконалення корпоративної системи захисту інформації з метою досягнення прийнятного

рівня захищеності інформаційних активів підприємства. Для цього необхідно:

- обґрунтувати і провести розрахунок фінансових вкладень в забезпечення безпеки на основі технологій аналізу ризиків, співвіднести витрати на забезпечення безпеки з потенційним збитком і ймовірністю його виникнення;
- виявити і провести першочергове блокування найбільш небезпечних вразливостей до здійснення атак на вразливі ресурси;
- визначити функціональні відносини і зони відповідальності при взаємодії підрозділів і посадових осіб щодо забезпечення інформаційної безпеки підприємства, створити необхідний пакет організаційно-розпорядчої документації;
- розробити і узгодити з службами організації, наглядовими органами проект впровадження необхідних комплексів захисту, що враховує сучасний рівень і тенденції розвитку інформаційних технологій;
- забезпечити підтримку впровадження комплексу захисту відповідно до умов роботи організації, що змінюються, регулярними доробками організаційно-розпорядчої документації, модифікацією технологічних процесів і модернізацією технічних засобів захисту.

Рішення названих завдань політик безпеки відкриває нові широкі можливості перед посадовими особами різного рівня.

Керівникам верхньої ланки це допоможе об'єктивно і незалежно оцінити поточний рівень інформаційної безпеки підприємства, забезпечити формування єдиної стратегії безпеки, розрахувати, узгодити і обгрунтувати витрати на захист компанії. На основі отриманої оцінки начальники відділів і служб зможуть виробити і обгрунтувати необхідні організаційні заходи (склад і структуру служби інформаційної безпеки, положення про комерційну таємницю, пакет посадових інструкцій та інструкції щодо дій в нештатних ситуаціях). Менеджери середньої ланки зможуть обгрунтовано вибрати засоби захисту інформації, а також адаптувати і використовувати в

своїй роботі кількісні показники оцінки інформаційної безпеки, методики оцінки та управління безпекою з прив'язкою до економічної ефективності підприємства.

Практичні рекомендації по нейтралізації та локалізації виявлених вразливостей системи, отримані в результаті аналітичних досліджень, допоможуть в роботі над проблемами інформаційної безпеки на різних рівнях і, що особливо важливо, допоможуть визначити основні зони відповідальності, в тому числі матеріальної, за неналежне використання інформаційних активів підприємства. При визначенні масштабів матеріальної відповідальності за шкоду, заподіяну роботодавцю, в тому числі пов'язаний з розголошенням комерційної таємниці, слід керуватися положеннями гл. 39 Трудового кодексу РФ.

Відповідно до ст. 20 Федерального закону «Про інформацію, інформатизації і захисту інформації» цілями захисту інформації є в тому числі: запобігання витоку, розкрадання, втрати, спотворення, підробки інформації; запобігання несанкціонованим діям зі знищення модифікації, спотворення, копіювання, блокування інформації; запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи.

Тому головною метою політик безпеки російських підприємств є забезпечення сталого функціонування підприємства: запобігання загрозам його безпеки, захист законних інтересів власника інформації від протиправних посягань, у тому числі кримінально караних діянь у даній сфері відносин, передбачених Кримінальним кодексом РФ, забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта. Інше завдання політик безпеки зводиться до підвищення якості послуг, що надаються і гарантій безпеки майнових прав та інтересів клієнтів.

Для цього необхідно:

- віднести інформацію до категорії обмеженого доступу (комерційної таємниці);

- прогнозувати і своєчасно виявляти загрози безпеки інформаційних ресурсів, причини та умови, що сприяють нанесенню фінансового, матеріального і морального збитку, порушення нормального функціонування і розвитку ресурсів;

- створити умови функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і нанесення різних видів шкоди;

- створити механізм і умови оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні автоматизованих систем, а також припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки;

- створити умови для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб і тим самим послабити негативний вплив наслідків порушення інформаційної безпеки.

При розробці політики розглядаються наступні об'єктивні фактори:

- загрози інформаційної безпеки, які характеризуються ймовірністю виникнення і ймовірністю реалізації;

- вразливості інформаційної системи або системи контрзаходів (системи інформаційної безпеки), що впливають на ймовірність реалізації загрози;

- ризик - фактор, що відображає можливий збиток підприємства в результаті реалізації загрози інформаційної безпеки: витоку інформації і її неправомірному використанню (ризик в кінцевому підсумку відображає ймовірні фінансові втрати - прямі або непрямі).

Таким чином, для створення ефективних політик безпеки російських підприємств пропонується спочатку провести аналіз ризиків в області інформаційної безпеки. Потім визначити оптимальний рівень ризику для підприємства на основі заданого критерію. Політику безпеки і відповідну корпоративну систему захисту інформації належить побудувати таким чином, щоб досягти заданого рівня ризику.

Запропонована методика розробки політики інформаційної безпеки сучасного підприємства дозволяє повністю проаналізувати і документально оформити вимоги, пов'язані з забезпеченням інформаційної безпеки, уникнути витрат на зайві заходи безпеки, можливі при суб'єктивній оцінці ризиків, надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем, забезпечити проведення робіт в стислі терміни, уявити обгрунтування для вибору заходів протидії, оцінити е фективность контрзаходів, порівняти різні варіанти контрзаходів.

В ході робіт повинні бути встановлені межі дослідження. З цією метою необхідно виділити вимагають оцінки ризиків ресурси інформаційної системи. При цьому належить розділити ресурси і зовнішні елементи, з якими здійснюється взаємодія. Ресурсами можуть бути кошти обчислювальної техніки, програмне забезпечення, дані, а також відповідно до ст. 2 Федерального закону «Про інформацію, інформатизацію і захист інформації» інформаційні ресурси - окремі документи і окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах). Прикладами зовнішніх елементів є мережі зв'язку (абз. 4 ст. 2 Федерального закону «Про зв'язок»), зовнішні сервіси і т.п.

При побудові політики будуть враховуватися взаємозв'язки між ресурсами. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв'язки визначають основу побудови моделі підприємства з точки зору інформаційної безпеки.

Ця модель, відповідно до запропонованої методики, будується наступним чином: для виділених ресурсів визначається їх цінність, як з точки зору асоційованих з ними можливих фінансових втрат, так і з точки зору шкоди репутації підприємства, дезорганізації її діяльності, моральної шкоди від розголошення конфіденційної інформації і т. д. Потім описуються

взаємозв'язки ресурсів, визначаються загрози безпеки і оцінюються ймовірності їх реалізації.

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, що знижують ризики до допустимих рівнів і володіють найбільшою цінової ефективністю. Частиною системи контрзаходів будуть рекомендації з проведення регулярних перевірок ефективності системи захисту.

Забезпечення підвищених вимог до інформаційної безпеки передбачає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів проводиться після завершення етапу аналізу ризиків та вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму інформаційної безпеки, політики інформаційної безпеки, сертифікація інформаційної системи (технології) на відповідність вимогам певному стандарту безпеки.

По завершенні робіт можна буде визначити міру гарантії безпеки інформаційного середовища, засновану на оцінці, з якої можна довіряти інформаційному середовищі об'єкта. Даний підхід передбачає, що більшу гарантію дає застосування великих зусиль при проведенні оцінки безпеки. Адекватність оцінки заснована на залученні в процес оцінки більшого числа елементів інформаційного середовища об'єкта; глибині, що досягається за рахунок використання при проектуванні системи забезпечення безпеки більшого числа проектів і описів деталей виконання; строгості, яка полягає в застосуванні більшого числа інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей або на зменшення ймовірності їх наявності.

Важливо пам'ятати, що перш ніж впроваджувати будь-які рішення щодо захисту інформації, необхідно розробити політику безпеки, адекватну цілям і завданням сучасного підприємства. Зокрема, політика безпеки повинна описувати порядок надання і використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях

безпеки. Система інформаційної безпеки виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політик безпеки, і навпаки. Етапи побудови необхідних політик безпеки - це внесення в опис об'єкта автоматизації структури цінностей, проведення аналізу ризику, визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації. При цьому політики безпеки бажано оформити у вигляді окремих документів і затвердити у керівництва підприємства.

В якості прикладу була досліджена політика інформаційної безпеки підприємства Softline (див.додаток Б). В ній відображені призначення, терміни, загальні положення, цілі задачі та принципи збезпечення ІБ, розподіл ролей та відповідальність за порушення ПІБ.

2.3 Практика формування політики інформаційної безпеки підприємства в Україні

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб.

Як показує практика формування політики інформаційної безпеки в Україні головними етапами побудови політики інформаційної безпеки є:

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

При цьому більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх

інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію).

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві:

- Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.
- Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.
- Підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.
- Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.
- Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.
- Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.
- Підсистема захисту систем управління базами даних.
- Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.
- Підсистема захисту мобільних пристроїв.

- Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них.

Як приклад політики ІБ розглядається комп'ютерна компанія «СофтСервіс» [7], у якій достатньо точно і чітко регламентуються всі моменти використання мережевого обладнання та програмного забезпечення. Для розуміння її сутності та призначення наводяться деякі витяги з цього нормативного документа. Мета політики ІБ полягає в тому, щоби гарантувати використання за призначенням комп'ютерної техніки і телекомунікаційних ресурсів підприємства її співробітниками, незалежними підрядниками та іншими користувачами. Всі користувачі корпоративної мережі мають використовувати комп'ютерні ресурси кваліфіковано, ефективно, дотримуючись норм етики і чинного законодавства.

Політика ІБ, її правила і умови стосуються всіх користувачів комп'ютерних і телекомунікаційних ресурсів і служб підприємства, де б ці користувачі не знаходилися. Порушення цієї політики тягне за собою дисциплінарні стягнення, аж до звільнення співробітника і/або притягнення його до кримінальної відповідальності. Політика ІБ може періодично змінюватись і переглядатися в міру потреби.

Керівництво підприємства має право, але не зобов'язане перевіряти будь-який або всі аспекти інформаційної системи, яка містить електронну пошту, з метою гарантувати дотримання політики ІБ. Комп'ютери та доступи до інформаційних ресурсів надаються співробітникам підприємства з метою допомогти їм більш ефективно виконувати свою роботу.

Комп'ютерна і телекомунікаційна системи належать підприємству і можуть використовуватися тільки в робочих цілях. Співробітники підприємства не повинні розраховувати на конфіденційність інформації, яку вони створюють, посилають або отримують за допомогою комп'ютерів і телекомунікаційних ресурсів, які належать підприємству. Користувачі мають

дотримувати умови всіх програмних ліцензій, авторське право і закони, що регулюють правовідносини у сфері інтелектуальної власності.

Користувачам комп'ютерів слід керуватися перерахованими нижче заходами щодо всіх комп'ютерних і телекомунікаційних ресурсів і служб підприємства, які містять таке обладнання: хост-комп'ютери, сервери файлів, робочі станції, автономні комп'ютери, мобільні комп'ютери, програмне забезпечення, а також внутрішні та зовнішні мережі (мережа Інтернет, комерційні інтерактивні служби і системи електронної пошти), до яких прямо або опосередковано звертаються комп'ютерні пристрої підприємства.

Невірні, нав'язливі, непристойні, наклепницькі, образливі, загрозливі або протизаконні матеріали забороняється пересилати електронною поштою або за допомогою інших засобів електронного зв'язку, а також відображати і зберігати їх на комп'ютерах підприємства. Користувачі, які помітили або отримали подібні матеріали, повинні негайно повідомити про цей інцидент своєму керівникові.

Все, що створене на комп'ютері підприємства, у т.ч. повідомлення електронної пошти та інші електронні документи, може бути проаналізовано керівництвом підприємства. Користувачі не мають права пересилати електронною поштою будь-які документи іншим особам і організаціям без дозволу відправника. Електронна пошта від юриста підприємства або адвоката, який представляє її інтереси, має містити в колонтитулі кожної сторінки повідомлення: «Захищено адвокатським правом/без дозволу не пересилати».

Користувачам не дозволяється встановлювати на комп'ютерах і в мережі підприємства власне програмне забезпечення без дозволу системного адміністратора. Користувачам забороняється змінювати і копіювати файли, що належать іншим користувачам, без дозволу власників файлів. Забороняється використання без попереднього письмового дозволу комп'ютерних і телекомунікаційних ресурсів і служб підприємства для передачі або зберігання комерційних або особистих оголошень, клопотань,

рекламних матеріалів, а також руйнівних програм, політичних матеріалів і будь-якої іншої інформації, на роботу з якою у користувача немає повноважень або призначеного для особистого використання.

Користувач несе відповідальність за збереження своїх паролів для входу в систему. Забороняється роздруковувати, зберігати в мережі або передавати іншим особам індивідуальні паролі. Користувачі несуть персональну відповідальність за всі транзакції, які будь хто зробить за допомогою їхнього пароля. Можливість входу в інші комп'ютерні системи через мережу підприємства не дає користувачам права на під'єднання до цих систем і використання їх без спеціального дозволу операторів цих систем.

Прийняття політики ІБ будь-якого підприємства та отримання підпису від кожного співробітника – кожен працівник зобов'язаний ознайомитися з політикою ІБ і підписатися під нею. Фактично, в нашому українському менталітеті тільки це змушує співробітників підприємства уважно прочитати і вникнути в зміст документа. А у випадку його порушення – тільки це дає законне юридичне право на відповідне стягнення з співробітника.

Отже, політика ІБ підприємства має містити такі рішення та заходи щодо її забезпечення:

- проведення аудиту ІБ та оцінювання захищеності інформаційних ресурсів підприємства, підготовка її інформаційних систем для досягнення відповідності чинних вимог щодо забезпечення ІБ;
- організація комплексної системи захисту інформації, яка знаходиться в інформаційно-управлінській системі виробничо-господарської діяльності підприємства, в яку внесено:

1. Комплексний захист від несанкціонованих доступів: управління доступом; реєстрація та облік подій ІБ; забезпечення контролю за цілісності та доступності інформаційних ресурсів; надійний криптографічний захист інформації;

2. Забезпечення ІБ міжмережевої взаємодії: проведення міжмережевого екранування та сегментації доступу до мереж; створення віртуальних приватних мереж; пошук і запобігання вторгнень та ін.;

3. Безпечний віддалений доступ до наявних корпоративних інформаційних ресурсів, в т.ч. конкретні мережі та мережі загального доступу;

4. Професійний контроль над використанням інформаційних ресурсів;

- захист інформаційно-управлінських систем спільно з:

1. Управлінням доступом на прикладному рівні, комплексним розробленням і реалізацією концепції повноважень користувачів;

2. Налаштуванням аудиту подій ІБ із під'єднанням до централізованих систем контролю над інцидентами;

3. Професійним захистом (безпечним налаштуванням) загальносистемного і спеціалізованого програмного забезпечення;

4. Захистом від несанкціонованого доступу, розмежуванням доступу;

- повне налаштування систем захисту інформації в інформаційних системах, які призначені для надійної обробки персональних даних;
- налаштування систем контролю та захисту інформації в автоматизованій системі управління;
- налаштування системи управління ідентифікаційними даними, централізованого управління доступом і забезпечення аутентифікації
- оперативна доставка і супровід засобів комп'ютерної техніки.

Отже, відповідальність за дотримання політики ІБ підприємства несе кожен його співробітник, при цьому першочерговим завданням є забезпечення безпеки всіх активів підприємства. Це означає, що інформація повинна бути захищена не менш надійно, ніж будь-який інший основний актив підприємства. Головні цілі компанії не можуть бути досягнуті без своєчасного і повного забезпечення співробітників інформацією, необхідною їм для виконання своїх службових обов'язків.

Висновки до другого розділу

Таким чином, у другому розділі були досліджені:

1. Кращі політики інформаційної безпеки європейських країн та Росії.
2. Практика формування політики інформаційної безпеки на сучасному українському підприємстві.

Результати досліджених питань можуть бути використанні для розробки рекомендацій щодо формування політики інформаційної безпеки підприємства.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ ШОДО ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1 Удосконалення методичних підходів до формування політики інформаційної безпеки

Серед основних факторів, що впливають на ефективність ПІБ, є успішність її розробки і впровадження. Наведені нижче рекомендації містять основні принципи створення ефективних політик.

1. Мінімізація впливу політики інформаційної безпеки на виробничий процес. Впровадження ПІБ практично завжди пов'язане зі створенням деяких незручностей для співробітників підприємства і зниженням продуктивності бізнес процесів. (Однак правильна система заходів ІБ підвищує ефективність бізнес процесів підприємства за рахунок значного підвищення рівня ІБ, що є одним з основних показників ефективності). Вплив заходів ІБ на бізнес процеси необхідно мінімізувати. У той же час не варто прагнути зробити заходи ІБ абсолютно прозорими. Для того щоб зрозуміти, який вплив політика буде надавати на роботу підприємства, і уникнути непорозумінь, слід залучати до розробки цього документа представників бізнес підрозділів, служб технічної підтримки і всіх, кого це безпосередньо торкнеться.

ПІБ - продукт колективної творчості [2]. Рекомендується включати до складу робочої групи наступних співробітників підприємства:

- керівника вищої ланки;
- керівника, відповідального для впровадження і контроль виконання вимог ПІБ;
- співробітника юридичного департаменту;
- співробітника служби персоналу;
- представника бізнес користувачів;
- технічного письменника;

- експерта з розробки ПІБ.

До складу робочої групи може входити від 5 до 10 осіб. Розмір робочої групи залежить від розміру підприємства і широти проблемної галузі, яку охоплює ПІБ.

2. Безперервність навчання. Навчання користувачів та адміністраторів інформаційних систем є найважливішою умовою успішного впровадження ПІБ. Тільки свідоме виконання вимог ПІБ приводить до позитивного результату. Навчання реалізується шляхом ознайомлення всіх користувачів з ПІБ під розпис, публікації ПІБ, розсилки користувачам інформаційних листів, проведення семінарів і презентацій, а також індивідуальної роз'яснювальної роботи з порушниками вимог ПІБ. У разі необхідності на порушників безпеки накладаються стягнення, передбачені ПІБ і правилами внутрішнього розпорядку. Користувачі інформаційних систем повинні знати кого, в яких випадках і яким чином треба інформувати про порушення ІБ. Однак це не повинно виглядати як доноси. Контактна інформація осіб, що відповідають за реагування на інциденти, повинна бути доступна будь-якому користувачеві.

3. Безперервний контроль та реагування на порушення безпеки. Контроль виконання правил ПІБ може здійснюватися шляхом проведення планових перевірок в рамках заходів з аудиту ІІБ. В підприємстві повинні бути передбачені заходи з реагування на порушення правил ПІБ. Ці заходи повинні передбачати оповіщення про інцидент, реагування, процедури відновлення, механізми збору доказів, проведення розслідування та притягнення порушника до відповідальності. Система заходів по реагуванню на інциденти, повинна бути скоординована між ІТ-департаментом, службою безпеки та службою персоналу. Політика повинна по можливості носити не рекомендаційний, а обов'язковий характер. Відповідальність за порушення політики повинна бути чітко визначена. За порушення ПІБ повинні бути передбачені конкретні дисциплінарні, адміністративні стягнення і матеріальна відповідальність.

4. Постійне вдосконалення політики інформаційної безпеки. ПІБ не є набором раз і назавжди визначених прописних істин. Не слід намагатися шляхом впровадження ПІБ вирішити відразу всі проблеми ІБ. Політика є результатом узгоджених рішень, що визначають основні вимоги щодо забезпечення ІБ і відображають існуючий рівень розуміння цієї проблеми в підприємстві. Для того щоб залишатися ефективною ПІБ повинна періодично коригуватися. Повинна бути визначена відповідальність за підтримання ПІБ в актуальному стані і призначені інтервали її перегляду. Політика повинна бути простою і зрозумілою. Слід уникати ускладнень, які зроблять політику непрацездатною. З цієї ж причини вона не повинна бути довгою. Інакше більшість користувачів не зможуть дочитати її до кінця, а, якщо і дочитають, то не пам'ятають про що в ній йдеться.

5. Підтримка керівництва підприємства. На етапі впровадження ПІБ вирішальне значення має підтримка керівництва підприємства. ПІБ вводиться в дію наказом керівника підприємства і процес її впровадження має перебуває у нього на контролі. В ПІБ повинна бути явно прописана заклопотаність керівництва питаннями забезпечення ІБ. З боку координатора робочої групи по розробці ПІБ керівництву підприємства повинні бути роз'яснені ризики, що виникають у разі відсутності ПІБ, а приписувані ПІБ заходи забезпечення ІБ повинні бути економічно обгрунтовані.

Розробка ПІБ - тривалий і трудомісткий процес, що вимагає високого професіоналізму, відмінного знання нормативної бази в області ІБ і, крім усього іншого, письменницького таланту. Цей процес зазвичай займає кілька місяців і не завжди завершується успішно. Координатором цього процесу є фахівець, на якого керівництво підприємства покладає відповідальність за забезпечення ІБ. Цей фахівець координує діяльність робочої групи з розробки та впровадження ПІБ протягом усього життєвого циклу, який складається з п'яти послідовних етапів [2], описаних нижче.

1. Початковий аудит безпеки. Аудит безпеки - це процес, з якого починаються будь-які планомірні дії щодо забезпечення ІБ в організації. Він

включає в себе проведення обстеження, ідентифікацію загроз безпеки, ресурсів, що потребують захисту та оцінку ризиків. В ході аудиту проводиться аналіз поточного стану ІБ, виявляються існуючі уразливості, найбільш критичні області функціонування і найбільш чутливі до погроз ІБ бізнес процеси.

2. Розробка. Аудит безпеки дозволяє зібрати і узагальнити відомості, необхідні для розробки ПІБ. На підставі результатів аудиту визначаються основні умови, вимоги і базова система заходів щодо забезпечення ІБ на підприємстві, що дозволяють зменшити ризики до прийнятної величини, які оформляються у вигляді узгоджених в рамках робочої групи рішень і затверджуються керівництвом підприємства. Розробка ПІБ з нуля не завжди є хорошою ідеєю. У багатьох випадках можна скористатися існуючими напрацюваннями, обмежившись адаптацією типового комплекту ПІБ до специфічних умов свого підприємства. Цей шлях дозволяє заощадити багато місяців роботи і підвищити якість розроблюваних документів. Крім того, він є єдино прийнятним у разі відсутності на підприємстві власних ресурсів для кваліфікованої розробки ПІБ.

3. Впровадження. З найбільшими труднощами доводиться стикатися на етапі впровадження ПІБ, яке, як правило, пов'язане з необхідністю вирішення технічних, організаційних та дисциплінарних проблем. Частина користувачів можуть свідомо, чи несвідомо чинити опір введенню нових правил поведінки, яких наразі необхідно дотримуватись, а також програмно-технічних механізмів захисту інформації, які в тій чи іншій мірі неминуче обмежують їх вільний доступ до інформації. Адміністраторів інформаційних систем може дратувати необхідність виконання вимог ПІБ, бо вони ускладнюють завдання адміністрування. Крім цього можуть виникати і чисто технічні проблеми, пов'язані, наприклад, з відсутністю в використовуваному ПО функціональності, необхідної для реалізації окремих положень ПІБ.

На етапі впровадження необхідно не просто довести зміст ПІБ до відома всіх співробітників підприємства, але також провести навчання і дати

необхідні роз'яснення тим, хто сумнівається, намагається обійти нові правила і продовжує працювати по-старому. Щоб впровадження завершилося успішно, повинна бути створена проектна група з впровадження ПІБ, що діє за узгодженим планом відповідно до встановлених термінів виконання робіт.

4. Аудит і контроль. Дотримання положень ПІБ повинно бути обов'язковою для всіх співробітників організації і має безперервно контролюватися. Проведення планового аудиту безпеки є одним з основних методів контролю працездатності ПІБ, що дозволяє оцінити ефективність впровадження. Результати аудиту можуть служити підставою для перегляду деяких положень ПІБ і внесення в них необхідних коригувань.

5. Перегляд і коригування. Перша версія ПІБ зазвичай не повною мірою відповідає потребам підприємства, однак розуміння цього приходить з досвідом. Швидше за все, після спостереження за процесом впровадження ПІБ і оцінки ефективності її застосування буде потрібно здійснити ряд доробок. На додаток до цього, використовувані технології і організація бізнес процесів безперервно змінюються, що призводить до необхідності коректувати існуючі підходи до забезпечення ІБ. У більшості випадків щорічний перегляд ПІБ є нормою, яка встановлюється самою політикою.

3.2 Формування універсальної структури політики інформаційної безпеки підприємства

Структура політики і її деталізація можуть відрізнятися, в залежності від особливостей підприємства, але вони повинні грунтуватися на типовій структурі, яка була сформована на основі політики підприємств EveryMatrix (див. додаток А) та Softline (див. додаток Б), та включає наступні розділи:

1. Введення.
2. Нормативні посилання.
3. Терміни та визначення.
4. Позначення та скорочення.

5. Область застосування.
6. Цілі та завдання.
7. Основні положення.
8. Об'єкти захисту.
9. Ризик і модель загроз інформаційній безпеці.
10. Модель порушника інформаційної безпеки.
11. Заходи інформаційної безпеки.
12. Реагування на інциденти інформаційної безпеки.
13. Забезпечення безпеки каналів зв'язку.
14. Розподіл відповідальності.
15. Порядок перегляду та актуалізації політики.

Крім того, політика може включати або містити посилання на наступні документи, які затверджуються в установленому порядку керівництвом підприємства:

1. Положення про локальну (корпоративної) мережі і по організації захищених мережевих з'єднань;
2. Положення про забезпечення інформаційної безпеки на рівні мережевий інфраструктури і межсетевое екранування;
3. Інструкція системного адміністратора локальної (корпоративної) мережі;
4. Положення про відділ забезпечення інформаційної безпеки (Інструкція адміністратора інформаційної безпеки) локальної (Корпоративної) мережі;
5. Положення по оновленню системного і прикладного програмного забезпечення, а також резервного копіювання та відновлення даних;
6. Інструкція по парольному захисту;
7. Інструкція з антивірусного захисту;
8. Інструкція по забезпеченню безпеки при роботі зі знімними носіями даних, мобільними пристроями, накопичувачами даних;

9. Правила по розробці матриці доступу до інформаційних ресурсів автоматизованої системи;

10. Перелік дозволеного до використання програмного забезпечення;

11. Інструкція по роботі з мережею Інтернет та корпоративною електронною поштою;

12. Порядок управління інформаційними активами підприємства;

13. Інструкція з організації технічного захисту інформації;

14. Інструкція з організації криптографічного захисту інформації;

15. Порядок поводження з інформацією, що підлягає захисту;

16. План забезпечення безперервної роботи та відновлення працездатності організації в надзвичайних (позаштатних) ситуаціях.

Вступ повинен включати в себе загальні відомості про підприємство.

Розділ «Нормативні посилання» повинен містити перелік всіх нормативних документів, на які є посилання в політиці.

У розділ «Терміни та визначення» необхідно включити всі використовувані в політиці терміни та визначення.

У розділ «Позначення та скорочення» необхідно включити всі використовувані в політиці позначення і скорочення.

У розділі «Область застосування» необхідно вказати сферу поширення документа і межі його дії.

У розділі «Цілі і завдання» необхідно привести основні цілі та завдання політики.

У розділі «Основні положення» необхідно відобразити принципи, методи і заходи забезпечення інформаційної безпеки на підприємстві.

У розділі «Об'єкти захисту» необхідно відобразити захищаються активи підприємства. До активів підприємства можна віднести наступні:

- персонал підприємства, інформаційні ресурси, чутливі по відношенню до випадкових і несанкціонованих дій і порушення їх безпеки, в тому числі, загальнодоступна інформація, представлена у вигляді документів і масивів інформації, незалежно від форми та виду їх подання;

- програмні ресурси - операційні системи та прикладне ПЗ, засоби розробки та утиліти, серверні додатки і сервіси;

- фізичні ресурси - комп'ютерне і комунікаційне обладнання, носії даних, приміщення та ін.

У розділі «Ризик і модель загроз інформаційній безпеці» необхідно привести основні принципи аналізу ризиків інформаційної безпеки на підприємстві, що пов'язані, в тому числі, із взаємодією зі сторонніми організаціями. Якщо доступ сторонніх організацій до інформаційних активів організації і засобів обробки інформації необхідний по виробничим причин, а також, в разі отримання товарів і послуг від сторонніх підприємств, слід проводити аналіз ризиків для визначення можливих наслідків для безпеки інформації і вимог до засобів управління. Ці заходи слід узгоджувати і визначати в договорах зі стороннім підприємством.

У розділі «Ризики інформаційної безпеки підприємства» слід визначити ризики по відношенню до інформації та засобів її обробки, що належить організації, з боку діяльності підприємства, в яких беруть участь сторони, перед наданням доступу слід впровадити прийнятні засоби управління. Якщо є необхідність у вирішенні доступу сторонніх підприємств до засобам обробки інформації та / або інформаційних активів підприємства, то для встановлення вимог до конкретних засобів управління слід визначити ризики. При визначенні ризиків, що відносяться до доступу сторонніх підприємств, слід брати до уваги:

- засоби обробки інформації, до яких потрібен доступ стороннього підприємства;

- тип доступу сторонньої організації до інформації та засобів її обробки, наприклад:

- фізичний доступ - до офісних приміщень, комп'ютерних кімнат, серверних;

- логічний доступ - до баз даних та інформаційних систем підприємства;

- мережеве з'єднання між мережами підприємства і стороннім підприємством - постійне з'єднання або віддалений доступ.

- чи надається доступ на місці експлуатації або поза ним;

- цінність і конфіденційність задіяної інформації, а також її чутливість для підприємства;

- засоби управління, необхідні для захисту інформаційних активів організації і не призначені для надання доступу стороннім підприємствам;

- персонал стороннього субпідрядника, який бере участь в обробці інформації підприємства;

- спосіб ідентифікації організації або персоналу, уповноважених отримувати доступ, спосіб перевірки повноважень, а також частоту підтвердження цієї потреби;

- різні способи і засоби управління, які використовуються сторонніми підприємствами для зберігання, обробки, передачі, спільного використання і обміну інформацією;

- вплив відмови в необхідному доступі до інформації на стороннього субпідрядника, а також введення і отримання їм неточної або тієї, що вводить в оману, інформації;

- практики і процедури, пов'язані з інцидентами інформаційної безпеки і потенційними збитками, терміни і умови продовження доступу стороннього підприємства в разі інциденту інформаційної безпеки;

- юридичні та нормативні вимоги, а також інші договірні зобов'язання, пов'язані з стороннім підприємством, які слід приймати до уваги;

- вплив угод на інтереси будь-яких інших зацікавлених сторін.

Підприємства можуть бути схильні до ризиків, пов'язаних з внутрішніми процесами управління комунікаціями підприємства, якщо застосовується високий ступінь аутсорсингу, або якщо задіяні кілька сторонніх підприємств.

Засоби управління описують угоди з різними сторонніми підприємствами, включаючи, наприклад:

- постачальників послуг, таких як провайдери мережі Інтернет, телефонні служби,

- експлуатаційні служби і служби підтримки;

- керовані служби безпеки;

- аутсорсинг засобів або операцій, наприклад, системи інформаційних технологій, сервіси накопичення інформації, центри обробки дзвінків;

- персонал, який здійснює підтримку і супровід апаратних засобів і програмного забезпечення;

- персонал, який здійснює прибирання, охорону, що забезпечує суспільне харчування та інші господарські служби;

- тимчасовий персонал, студенти та особи, які працюють за трудовими угодами (клієнти).

Дані угоди можуть допомогти знизити ризики, пов'язані зі сторонніми підприємствами.

Розділ «Загрози інформаційної безпеки». Потенційні загрози інформаційній безпеці по природі їх виникнення поділяються на два типи: природні (об'єктивні) і штучні (суб'єктивні).

Джерела загроз по відношенню до самої інформаційної системи можуть бути як зовнішніми, так і внутрішніми. Існують наступні види загроз інформаційній безпеці:

1. Загрози порушення конфіденційності: розкрадання (витік, перехоплення), втрата (ненавмисна втрата), розголошення інформації як умисне, так і ненавмисне;

2. Загрози порушення цілісності інформації: модифікація (спотворення) інформації, заперечення автентичності інформації, нав'язування неправдивої інформації;

3. Загрози порушення доступності інформації: блокування інформації, знищення інформації і засобів її обробки та зберігання.

В якості джерел загроз можуть виступати як суб'єкти (особистість), так і об'єктивні прояви. Джерела загроз можуть перебувати як усередині об'єкта інформатизації - внутрішні, так і поза ним - зовнішні.

Всі джерела погроз діляться на класи, обумовлені типом носія загрози (джерела загрози):

- джерела загроз, обумовлені діями суб'єкта (людський фактор), які можуть бути кваліфіковані як умисні або випадкові провини;
- техногенні джерела загроз, обумовлені технічними засобами і визначаються технократичною діяльністю людини;
- стихійні джерела загроз, обумовлені природними явищами, які неможливо передбачити або можливо передбачити, але неможливо запобігти при сучасному рівні знаннь і можливостей.

У розділі «Порушники інформаційної безпеки» наводиться класифікація порушників безпеки інформації.

Порушники інформаційної безпеки за своєю приналежністю поділяються на дві групи: внутрішні і зовнішні. Під внутрішніми потенційними порушниками матися на увазі персонал підприємства, що має санкціонований доступ на територію об'єктів інформатизації. Під зовнішніми потенційними порушниками маються на увазі всі інші особи.

У розділі «Заходи інформаційної безпеки» необхідно вказати, які заходи застосовуються в частині організації процесу забезпечення інформаційної безпеки, а також процесу дотримання та виконання принципів і вимог політики. Основні заходи забезпечення інформаційної безпеки підприємства підрозділяються на:

- правові заходи;
- морально-етичні заходи;
- організаційні заходи;
- технологічні заходи;
- інженерно-технічні заходи;
- програмно-апаратні заходи;

- заходи безпеки у відносинах із зовнішніми користувачами.

До правових заходів інформаційної безпеки відносяться закони України, та інші нормативно-правові акти, що регламентують правила поводження з інформацією, що закріплюють права і обов'язки учасників інформаційних відносин у процесі її обробки і використання, а також встановлюють відповідальність за порушення цих правил.

До морально-етичних заходів належать норми поведінки, які традиційно склалися або складаються в міру поширення інформаційних технологій в колективі підприємства. Ці норми здебільшого не є обов'язковими, як законодавчо затверджені нормативні акти, однак, їх недотримання може привести до падіння авторитету, престижу людини, групи осіб або в цілому організації. Морально-етичні норми бувають як неписані, так і писані, тобто оформлені в певний звід (статут) правил чи приписів. Морально-етичні заходи захисту є профілактичними і вимагають постійної роботи по створенню здорового морального клімату в колективі підприємства.

Організаційні заходи в основному орієнтовані на роботу з персоналом, вибір місця розташування і розміщення об'єктів захисту, організацію систем фізичного, протипожежного захисту, контролю виконання вжитих заходів, покладання персональної відповідальності за виконання заходів захисту. Заходи застосовуються для зменшення числа внутрішніх антропогенних, техногенних і стихійних джерел загроз. Основними організаційними заходами є:

- вибір місця розташування і розміщення об'єкта інформатизації;

- фізичний захист і організація охорони;

- обмеження доступу в приміщення, в яких встановлені технічні засоби обробки інформації;

- підбір та робота з співробітниками;

- підвищення професійний кваліфікації співробітників;

- організація інструктажу персоналу;

- організація обліку обладнання і носіїв;
- контроль виконання вимог щодо захисту;
- протипожежна охорона;
- забезпечення надійного сервісного обслуговування;
- організація взаємодії з іншими підрозділами і підприємствами.

Усунення загроз організаційними методами є найменш витратним заходом щодо захисту інформації.

До технологічних заходів захисту відносяться різного роду технологічні рішення і прийоми, засновані на використанні деяких видів надмірності (структурної, функціональної, інформаційної, тимчасової і т.п.) і спрямовані на зменшення можливості здійснення співробітниками помилок і порушень в рамках наданих їм прав та повноважень.

До даних заходів належать:

- використання процедур подвійного введення відповідальної інформації;
- ініціалізації відповідальних операцій тільки при наявності погодження декількох осіб;
- процедури перевірки реквізитів вихідних і вхідних повідомлень і т.п.

Інженерно-технічні методи орієнтовані на оптимальну побудову будівель, споруд, інженерних мереж і транспортних комунікацій з урахуванням вимог забезпечення інформаційної безпеки.

До інженерно-технічних заходів належать:

- забезпечення електрозахисту устаткування і будівель;
- екранування приміщень;
- захист приміщень від руйнувань;
- оптимальне розміщення устаткування;
- оптимальне розміщення інженерних комунікацій;
- застосування засобів візуального захисту;
- акустична обробка приміщень;
- застосування систем кондиціонування.

Технічні заходи засновані на застосуванні спеціальних технічних засобів захисту інформації, контролю обстановки і орієнтовані на усунення загроз, пов'язаних з діями зовнішніх загроз по впливу на інформацію технічними засобами. Деякі з цих заходів дозволяють усунути вплив техногенних джерел загроз і послаблюють вплив об'єктивних, суб'єктивних і випадкових вразливостей.

До технічних заходів належать:

- резервування технічних засобів обробки;
- резервування каналів зв'язку;
- використання виділених каналів зв'язку;
- створення резервної копії (дублювання) інформаційних ресурсів;
- створення системи просторового зашумлення;
- створення системи акустичного і вібраційного зашумлення;
- екранування вузлів і устаткування;
- використання джерел гарантованого живлення;
- контроль каналів зв'язку для передачі інформації;
- контроль відсутності електронних пристроїв перехоплення інформації на об'єктах інформатизації.

Програмно-апаратні заходи призначені для усунення прояву загроз, безпосередньо пов'язаних з процесом обробки інформації. Реалізація програмно-апаратних заходів істотно знижує вплив внутрішніх антропогенних джерел загроз.

У групі програмно-апаратних заходів об'єднуються такі заходи, як:

- обмеження доступу до засобів обробки інформації (ПО, технічних засобів);
- обмеження доступу до об'єктів захисту (інформації, що захищається);
- розмежування доступу суб'єктів (користувачів);
- управління зовнішніми і внутрішніми потоками інформації;
- приховування структури і призначення;
- підтвердження достовірності інформації;

- перетворення (шифрування, кодування) інформації при її передачі і зберіганні;
- блокування невикористовуваних сервісів;
- моніторинг цілісності ПО, конфігурації ПО і апаратних засобів;
- антивірусний захист;
- моніторинг подій та інцидентів інформаційної безпеки;
- моніторинг дій користувачів корпоративної мережі.

При наданні стороннім особам доступу до інформації та активів підприємства, слід звертати увагу на відповідні вимоги інформаційної безпеки та вжити заходів безпеки у відносинах із зовнішніми користувачами.

Перед наданням доступу стороннім особам до будь-яких активів підприємства слід врахувати наступні умови, які стосуються інформаційної безпеки (в залежності від типу і рівня наданого доступу, з яких не всі можуть бути застосовані):

1. Захист активів, що включає:
- процедури визначення факту компрометації активів, наприклад, внаслідок втрати або модифікації даних;
- цілісність активів;
- обмеження на дублювання або розкриття інформації інформації;
- опис наданих товарів і послуг;
- різні передумови, вимоги і вигоди від доступу клієнтів;

2. Угоди з управління доступом, що охоплюють:
- дозволені методи доступу, а також управління і використання унікальних ідентифікаторів користувачів і паролів;
- процес надання привілеїв і повноважень на доступ;
- принцип заборони будь-якого доступу, явно недозволеного;
- процес відкликання прав доступу користувачів або блокування доступу;

- процедури звітності, повідомлення та розслідування інцидентів порушення інформаційної безпеки та виявлення слабких ланок системи безпеки;

- опис кожного сервісу, призначеного для доступу;

- плановий рівень сервісу і неприпустимі рівні сервісу;

- право моніторингу та скасування будь-якої діяльності, пов'язаної з активами підприємства;

- відповідні зобов'язання організації і клієнта;

- обов'язки, що стосуються юридичних питань і способів забезпечення відповідності вимогам законодавства, наприклад, законів про захист даних, беручи до уваги різні національні законодавчі системи, в разі, якщо угода включає співпрацю з клієнтами за кордоном;

- права на інтелектуальну власність і авторські права, а також захист будь-якої спільної роботи.

Вимоги інформаційної безпеки, які стосуються співробітників сторонніх підприємств, які отримують доступ до активів підприємства, можуть значно відрізнятися в залежності від класифікації наданої інформації і засобів її обробки. Дані вимоги безпеки можуть бути відображені в контракті, що укладається з співробітником стороннього підприємства, який містить всі певні ризики і вимоги інформаційної безпеки.

Контракт зі сторонніми підприємства також може містити і інші вимоги безпеки. У контракті на надання доступу стороннього підприємства, необхідно вказувати дозвіл на залучення інших прийнятних сторін, а також умови їх доступу та участі.

Розділ «Реагування на інциденти інформаційної безпеки» повинен містити опис процесу реагування на інциденти інформаційної безпеки, який повинен включати засоби системного аудиту для автоматизованих ділянок обробки інформації, а також регламент подання звітів про інциденти в області інформаційної безпеки для всього персоналу підприємства та іншу інформацію про стан системи захисту.

В даному розділі повинні бути описані механізми реагування на інциденти, наприклад, інформація про виявлення інцидентів порушення інформаційної безпеки доповідається керівництву і повідомляється адміністратору інформаційної безпеки в установленому порядку. Забороняється прийняття самостійних і несанкціонованих дій, які не регламентованих документами на підставі відповідної інструкції. При виявленні каналів витоку інформації, проводяться заходи по локалізації ділянки обробки інформації з метою припинення подальшої витоку, а також припиняються процеси, пов'язані з обробкою інформації, що захищається на підприємстві. У разі зараження шкідливими програмами проводяться заходи щодо усунення завданої шкоди, відповідно до «Інструкції по антивірусного захисту підприємства».

З метою ефективного управління інцидентами на підприємстві, в даному розділі слід описати обов'язки і порядок ефективної невідкладної обробки подій і слабких місць інформаційної безпеки. Як реакція на них слід застосовувати процеси безперервного вдосконалення, відстеження, оцінки та повного управління інцидентами інформаційної безпеки.

Для забезпечення швидкого, ефективного та організованого реагування на інциденти інформаційної безпеки, слід розробити і затвердити порядок управління інцидентами. Для виявлення інцидентів інформаційної безпеки, крім повідомлень про події та вразливості інформаційних систем, слід здійснювати моніторинг систем, оповіщень і вразливостей. Цілі управління інцидентами інформаційної безпеки необхідно узгоджувати з керівництвом, доводити до відома персоналу, що відповідають за управління інцидентами інформаційної безпеки, пріоритетів підприємства щодо поводження з інцидентами.

Інциденти інформаційної безпеки можуть виходити за рамки підприємства. Необхідно встановити механізм координації всіх дій, пов'язаних з реагуванням на інциденти, навіть якщо це стосується питання обміну інформацією про дані інциденти з зовнішніми підприємствами.

Розділ «Забезпечення безпеки каналів зв'язку». Захист дротових каналів зв'язку повинен бути спрямований на зниження ймовірності несанкціонованого доступу до інформації шляхом гальванічного підключення до інформаційних кабелів або зняття інформації через побічні електромагнітні випромінювання і наводки на інші кабелі, а також на забезпечення захисту кабельного обладнання від електромагнітних завад і механічного ушкодження.

Захист бездротових каналів зв'язку повинен бути спрямований на зниження таких атак, як прослуховування трафіку, відмова в обслуговуванні, несанкціоноване підключення.

Розділ «Розподіл відповідальності». Даний розділ є одним з важливих розділів політики і повинен відображати принципи управління інформаційної безпеки підприємства з боку керівництва, розподіл обов'язків, а також координацію питань інформаційної безпеки. Всі обов'язки по забезпеченню інформаційної безпеки повинні бути чітко визначені в даному розділі.

Основними обов'язками керівництва підприємства при забезпеченні інформаційної безпеки є:

- визначення цілей забезпечення інформаційної безпеки, відповідних вимогам підприємства;
- формулювання, перегляд та затвердження політики;
- контроль ефективності впровадження політики;
- забезпечення чіткого керівництва і відчутною адміністративної підтримки ініціативам, спрямованим на підвищення безпеки;
- виділення необхідних коштів інформаційної безпеки;
- призначення відповідальних за інформаційну безпеку в межах організації та їх обов'язки;
- ініціювання планів і програм підтримки обізнаності персоналу з інформаційної безпеки.

Крім того, необхідно здійснювати такі заходи:

- встановити і чітко визначити обов'язки відповідального персоналу, пов'язані з кожними окремими інформаційними системами і ресурсами, а також осіб, контролюючих їх дії;

- призначити відповідального за кожен актив і процес безпеки, а також задокументувати дані обов'язки;

- розмежувати повноваження відповідального персоналу та затвердити в установленому порядку;

- визначити критичні активи та процеси безпеки, а також документувати їх.

Необхідно призначити відповідального з числа керівництва підприємства, який буде відповідати за всі питання, пов'язані із забезпеченням інформаційної безпеки на підприємстві.

Керівникам різних зацікавлених підрозділів організації слід координувати питання впровадження заходів з управління інформаційною безпекою. Координація питань інформаційної безпеки повинна включати взаємодію і співпрацю керівництва, користувачів, адміністраторів, розробників додатків, аудиторів і персоналу безпеки, а також фахівців з навичками в таких областях, як страхування, юриспруденція, кадрова робота, управління інформаційними технологіями або ризиками. З урахуванням цього в даному розділі політики слід відобразити заходи щодо:

- оцінки заходів інформаційної безпеки на відповідність до затвердженої політики;

- визначення способів обробки випадків несумісності;

- утвердження методології і процесів забезпечення інформаційної безпеки, наприклад, визначення ризиків, класифікації інформації;

- визначення значущих змін загроз і моменів, коли інформація і засоби її обробки піддаються загрозам;

- оцінки адекватності та координації впровадження засобів управління інформаційною безпекою;

- ефективності обраного в масштабах підприємства навчання, тренінгів і обізнаності з питань інформаційної безпеки;

- аналізу інформації, отриманої в результаті виявлення та обробки інцидентів інформаційної безпеки, а також рекомендувати прийнятні заходи у відповідь на встановлені інциденти інформаційної безпеки.

В даному розділі також необхідно визначити механізми підписання і перегляду угод про дотримання конфіденційності, розробленого на підставі діючої на підприємстві політики.

Угоди про дотримання конфіденційності повинні відповідати вимогам щодо захисту конфіденційної інформації, закріпленим в нормативно-правових актах. При визначенні вимог до угод про дотримання конфіденційності слід керуватися наступними аспектами:

- класифікація інформації, що захищається (наприклад, конфіденційна інформація);

- очікуваний термін дії угоди, включаючи випадки, коли дотримання конфіденційності може бути безстроковим;

- необхідні заходи, в разі припинення дії угоди;

- відповідальність і дії осіб, які підписують угоду, щоб уникнути несанкціонованого розголошення інформації (такі як «принцип необхідного знання», «знати тільки те, що необхідно»);

- обов'язки і права осіб, які підписують угоду, при допуску до використання конфіденційної інформації;

- проведення аудиту і моніторингу використання конфіденційної інформації;

- порядок донесення і звітності про випадки несанкціонованого розголошення і порушень конфіденційності;

- визначення термінів, коли інформація повинна бути знищена або повернена, в разі припинення дії угоди;

- вживані заходи, в разі порушення угоди.

На підставі вимог політики, на підприємстві може виникнути необхідність в інших угодах про дотримання конфіденційності і нерозголошення. Угоди про дотримання конфіденційності і нерозголошення повинні відповідати чинним вимогам.

Вимоги до угод про дотримання конфіденційності інформації слід при необхідності (при зміні чинного законодавства) переглядати.

Угоди про дотримання конфіденційності призначені для захисту інформаційних активів підприємства. Особи, що підписують ці угоди, несуть відповідальність за несанкціоноване використання та розголошення конфіденційної інформації.

При різних обставинах підприємству можуть знадобитися різні форми угод про дотримання конфіденційності, але всі вони повинні відображати основні вимоги інформаційної безпеки.

Розділ «Порядок перегляду та актуалізації політики» визначає процедуру щодо перегляду та актуалізації політики, а також порядок внесення змін в політику. Також в даному розділі наводиться інформація (вид документа, реєстраційний номер та інші атрибути документа) про погодження.

Висновки до третього розділу

Таким чином, у третьому розділі були розроблені рекомендації щодо вдосконалення методичних підходів до формування політики інформаційної безпеки та універсальної структури політики інформаційної безпеки підприємства.

При розробці політики інформаційної безпеки варто пам’ятати:

1. Малоймовірно, що вийде написати документ, однаково придатний для заступника голови правління, начальника відділу системного адміністрування і рядового співробітника складу.

2. Цільова аудиторія політики безпеки - це керівники і фахівці IT-служби, відділу захисту інформації, проектного офісу, інші ключові користувачі, так чи інакше пов'язані з розробкою, впровадженням і підтримкою IT-систем та підрядники і консультанти, що виконують схожі функції на замовлення підприємства.

3. Добре написані терміни та визначення дають чітке уявлення про предмет і роблять більш зрозумілими всі висунуті в тексті вимоги.

4. Мінімальний набір тем, які має сенс відобразити в розроблюваної політики:

- Організаційна структура ІБ і об'єкти захисту (хто, що і чому захищає - про ризики, класифікацію активів, розподіл ролей і обов'язків).
- Контроль доступу (по суті, правила взаємодії учасників процесу і об'єктів захисту).
- Управління змінами (про те, як наші системи повинні безпечно і контрольовано переходити з одного стану в інший).
- Моніторинг і аудит (способи оцінки і підтвердження поточного стану захищеності).

ВИСНОВКИ

У результаті роботи було:

1. Проаналізовано вимоги нормативних документів та підходи до розробки політики інформаційної безпеки. Відповідно до міжнародних стандартів, політика інформаційної безпеки підприємства повинна відповідати наступним вимогам:

- бізнес-стратегії підприємства;
- правилам, законодавству та договорам;
- поточним та прогнозованим загрозам навколишнього середовища щодо інформаційної безпеки.

Порядок розробки політики інформаційної безпеки розділяється на наступні етапи:

Перший етап - початковий аудит безпеки, в тому числі проведення попереднього обстеження та інвентаризація стану інформаційної безпеки, ідентифікація загроз безпеки підприємства; ідентифікація ресурсів, потребують захисту; визначення ризиків.

Другий етап - розробка проекту політики інформаційної безпеки підприємства.

Третій етап - узгодження і запровадження в дію політики інформаційної безпеки підприємства.

2. Досліджено практику розробки політики інформаційної безпеки в різних країнах. В даний час сформувалася певна практика політик інформаційної безпеки. Це перш за все практика розробки політик, процедур, стандартів і керівництв безпеки таких визнаних технологічних лідерів як IBM, Sun Microsystems, Cisco Systems, Microsoft, Symantec, SANS та ін.

Як показує практика формування політики інформаційної безпеки в Україні головними етапами побудови політики інформаційної безпеки є:

- реєстрація всіх ресурсів, які мають бути захищені;
- аналіз та створення переліку можливих загроз для кожного ресурсу;

- оцінка ймовірності появи кожної загрози;
- вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему.

3. Розроблено рекомендації щодо удосконалення методичних підходів до формування політики інформаційної безпеки підприємства. Серед основних факторів, що впливають на ефективність ПІБ, є успішність її розробки і впровадження. Наведені нижче рекомендації містять основні принципи створення ефективних політик:

- Мінімізація впливу політики інформаційної безпеки на виробничий процес.
- Безперервність навчання.
- Безперервний контроль та реагування на порушення безпеки.
- Постійне вдосконалення політики інформаційної безпеки.
- Підтримка керівництва підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексеев Е. Г. Разработка политики информационной безопасности / Е. Г. Алексеев, С. Д. Богатырев [Електронний ресурс]. – Режим доступу: http://inf.e-alekseev.ru/text/Politics_inf_bezopas.html
2. Астахов А. Разработка эффективных политик информационной безопасности / А. Астахов [Електронний ресурс]. – Режим доступу: https://www.osp.ru/cio/2004/01/173121/
3. Березюк Л. П. Организационное обеспечение информационной безопасности: навч. посібник / Л. П. Березюк. – Хабаровськ : ДВГУПС, 2012. – 188 с.
4. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К.: «МК-Прес», 2015. – 432с.
5. Братель О. Поняття та зміст доктрини інформаційної безпеки / О. Братель // Право України. – 2017. – № 5. – С. 36-40.
6. Грибунин В. Г. Разработка и реализация политики безопасности предприятия / В. Г. Грибунин [Електронний ресурс]. – Режим доступу: http://www.bre.ru/security/22754.html
7. Грицюк Ю. І. Особливості організації інформаційної безпеки корпоративної мережі промислової компанії / Ю. І. Грицюк [Електронний ресурс]. – Режим доступу: http://nltu.edu.ua/nv/Archive/2013/23_4/314_Mil.pdf
8. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. – 2013. – № 5. – С. 2-3.
9. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К.: ООО «ТИД «ДС», 2014. – 992 с.
10. Домарев В. В. Створення підрозділу захисту інформації / В. В. Домарев [Електронний ресурс]. – Режим доступу: http://www.trn.ua/articles/2101/

11. Етапи побудови КСЗІ [Електронний ресурс]. – Режим доступу: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi
12. Жабинець О. Й. Політика інформаційної безпеки страхових компаній: українські реалії та досвід США / О. Й. Жабинець [Електронний ресурс]. – Режим доступу: http://www.problecon.com/export_pdf/problems-of-economy-2014-4_0-pages-22_27.pdf
13. Зайцев С. Е. Политики информационной безопасности в системах информационной безопасности / С. Е. Зайцев [Електронний ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/politiki-informatsionnoy-bezopasnosti-v-sistemah-informatsionnoy-bezopasnosti
14. Захаров Е. Информационная безопасность или опасность отставания / Е. Захаров // Права людини. – 2010. – № 1 . – С. 3-5.
15. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия: монографія / В. А. Игнатьев. – Старий Оскол: ООО «ТНТ», 2015. – 448 с.
16. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с..
17. Конеев И. Политики информационной безопасности / И. Конеев [Електронний ресурс]. – Режим доступу: https://www.osp.ru/cio/2007/11/4569379/
18. Корнюшин П.Н. Информационная безопасность / П. Н. Корнюшин, С. С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2013. – 154 с.
19. Корчагин И. Политика безопасности организации. Современный подход / И. Корчагин [Електронний ресурс]. – Режим доступу: http://bis-expert.ru/articles/43813
20. Маракова І. Захист інформації: підручник / І. Маракова, А. Рибак, Ю. Ямпольский – Одеса: ОдНПУ, 2011. – 164 с.

21. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Д. Матиев [Електронний ресурс]. – Режим доступу: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/
22. Медведев Н. В. Стандарты и политика информационной безопасности автоматизированных систем / Н. В. Медведев, П. М. Квасов, В. Л. Цирлов [Електронний ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/standarty-i-politika-informatsionnoy-bezopasnosti-avtomatizirovannyh-sistem.pdf
23. Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан [Електронний ресурс]. – Режим доступу: http://nics.gov.uz/upload/medialibrary/e6b/e6b3bd4d379464ddda22ac2ca262184e.pdf
24. Петренко С. А. Политики безопасности компании при работе в Интернет / С. А. Петренко, В. А. Курбатов [Електронний ресурс]. – Режим доступу: https://profilib.com/chtenie/140515/sergey-petrenko-politiki-bezopasnosti-kompanii-pri-rabote-v-internet.php
25. Политика информационной безопасности – опыт разработки и рекомендации [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/174489/
26. Політика інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://ua.kursoviks.com.ua/metodychni_vkazivky/article_post/806-lektsiya-26-na-temu-politika-informatsiynoi-bezpeki-z-kursu-zakhist-ta-bezpeka-informatsiynikh-resursiv-nudpsu
27. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22.05.98 № 505.

28. Постанова Кабінету Міністрів України від 04.07.2001 № 756 "Про затвердження переліку документів, які додаються до заяви про видачу ліцензії для окремого виду господарської діяльності".
29. Постанова Кабінету Міністрів України від 14.11.2000 № 1698 "Про затвердження переліку органів ліцензування".
30. Постанова Кабінету Міністрів України від 25.05.2011 № 543 "Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню".
31. Постанова Кабінету Міністрів України від 25.05.2011 № 616 "Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення".
32. Постанова Кабінету Міністрів України від 29.10.2000 № 1755 "Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу".
33. Разработка политики информационной безопасности [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/20_AND_2014/Informatica/4_174328.doc.htm
34. Скрипник Д. А. Управление непрерывностью услуг и информационной безопасностью в рамках этапа Проектирования. Управление поставщиками, ITIL. IT Sevice Management по стандартам V.3.1, 2012 / Д. А. Скрипник [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/studies/courses/2323/623/lecture/13567?page=3
35. Чубарук Т. Проблеми законодавчого забезпечення інформаційної безпеки в Україні / Т. Чубарук // Право України. – 2017. – № 9. – С. 67–69
36. Чунарьова А. В. Управління інформаційною безпеки сучасних ІКСМ на базі міжнародних стандартів ISO, Національний авіаційний університет (НАУ) / А. В. Чунарьова, А. В Чунарьов. [Електронний ресурс]. –

Режим доступу: http://www.rusnauka.com/20_PNR_2010/Informatica/70334.doc.htm

37. Щебланін Ю. М. Правове забезпечення інформаційної безпеки / Ю. М. Щебланін [Електронний ресурс]. – Режим доступу: http://www.studfiles.ru/preview/5367198/page:4/#5367198
38. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ [Текст] / В. М. Щербина // Актуальні проблеми економіки. – 2016. – № 10. – С. 220-225.
39. Юдін О.К. Захист інформації в мережах передачі даних: Підручник / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.
40. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management
41. ISO/IEC 20000:2005. Information technology. Service management. Part 2: Code of practice/
42. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements
43. ISO/IEC TR 18044:2004. Information technology -Security techniques - Information security incident management/

ДОДАТКИ

Додаток А

Політика інформаційної безпеки підприємства EveryMatrix

Цілі інформаційної безпеки

Метою підприємства EveryMatrix в галузі управління інформаційною безпекою є забезпечення здійснення її основних і допоміжних видів комерційної діяльності з мінімальною кількістю збоїв.

Підприємство EveryMatrix зобов'язане гарантувати абсолютну цілісність і доступність всієї інформації, яка зберігається або використовується ним. Підприємство EveryMatrix зобов'язане забезпечити використання і зберігання всієї відповідної інформації з дотриманням належних процедур з точки зору конфіденційності.

Політика інформаційної безпеки

Метою даної політики є забезпечення захисту інформаційних активів підприємства від будь-яких, внутрішніх або зовнішніх, навмисних або випадкових, загроз.

Політика щодо системи управління інформаційною безпекою (СУІБ) затверджена генеральним директором підприємства EveryMatrix.

Метою даної Політики є:

- Надання інформації співробітникам і представникам громадськості з мінімальними перебоями і відповідно до вимог бізнес-процесу. Це дозволяє забезпечити доступність інформації та важливих послуг для користувачів у відповідний час і у відповідному місці.

- При цьому забезпечується цілісність такої інформації. Це означає забезпечення достовірності і повноти інформації за допомогою захисту від несанкціонованих змін.

- Забезпечення конфіденційності інформації, але не обмежуючись даними досліджень, інформацією третіх осіб, особистими даними та електронними повідомленнями. Це дозволяє забезпечити захист цінної або секретної інформації від несанкціонованого розголошення або неминучих перебоїв в доступі.

- Дотримання нормативних і законодавчих вимог. Це дозволяє забезпечити дотримання з боку підприємства вимог відповідних комерційних, національних і міжнародних нормативно-правових та законодавчих актів.

- З метою запобігання збоїв в процесі здійснення комерційної діяльності та забезпечення захисту важливих бізнес-процесів від наслідків серйозних збоїв або несправностей, надається Програма управління підвищенням стійкості функціонування підприємства, а також складаються плани по підвищенню стійкості функціонування підприємства. Складання і перевірка планів щодо підвищення стійкості функціонування підприємства.

- Підвищення рівня освіченості та поінформованості, а також навчання персоналу і відповідних третіх осіб у сфері інформаційної безпеки.

- Дані про всі, фактичні або передбачувані, випадки порушення інформаційної безпеки надається відповідним органам і розслідується їх представниками, не обмежуючись тільки процесом реагування на інциденти.

- Здійснення належного контролю над доступом і забезпечення захисту інформації від несанкціонованого доступу.

Ризики, пов'язані з СУІБ

У підприємства EveryMatrix управління інформаційної безпеки здійснюється на основі програми управління ризиками.

З метою забезпечення підтримки реалізації Політики щодо СУІБ політики, процедури і методичні рекомендації без обмежень надаються в роздрукованому вигляді, а також в електронному вигляді через внутрішню мережу.

Відповідальність

Кожен співробітник несе відповідальність за дотримання вимог Політики щодо СУІБ. Всі керівники несуть безпосередню відповідальність за впровадження Політики щодо СУІБ в рамках своїх підрозділів, а також за дотримання її вимог власними співробітниками.

Відповідно до цього документа керівником служби безпеки призначається представник керівництва п-н Раду Попеску (Radu Popescu), який несе безпосередню відповідальність за розробку, планування, впровадження та експлуатацію СУІБ на підприємстві EveryMatrix. Він також бере участь у складанні і (або) управлінні процесом розробки відповідних

політик, процедур і методичних рекомендацій, що відносяться до інформаційної безпеки.

Підрозділ внутрішнього аудиту несе безпосередню відповідальність за перевірку ефективності Політики щодо СУІБ.

Політика щодо СУІБ підлягає перегляду в разі істотних змін в підприємстві.

Додаток Б

Політика інформаційної безпеки підприємства Softline

1. Призначення

1.1. Політика інформаційної безпеки є основним документом, що регулює діяльність підприємства Softline в області інформаційної безпеки.

1.2. Корпоративні вимоги в сфері забезпечення інформаційної безпеки поширюються на всі регіони діяльності і на всі бізнес-підрозділи підприємства Softline.

2. Терміни та визначення, скорочення і позначення

2.1. терміни та визначення

Аудит - систематичний, незалежний і задокументований процес отримання доказів аудиту і їх об'єктивного оцінювання для визначення ступеня відповідності критеріям аудиту.

Підприємство - будь-яка юридична особа, що входить до групи підприємств Софтлайн або афілійована з ними.

Корпоративна культура підприємства - це звід важливих положень діяльності підприємства, які визначаються його місією і стратегією розвитку і знаходять вираження в сукупності соціальних норм і цінностей, поділюваних усіма співробітниками підприємства.

Працівник - фізична особа, яка перебуває у трудових відносинах з підприємством на підставі укладеного трудового договору і працює в ньому за основним місцем роботи, або за сумісництвом.

Співробітник - фізична особа, яка вступила в трудові відносини з роботодавцем.

2.2. Скорочення і позначення

ПІБ - прізвище, ім'я, по батькові. Ім'я та по батькові вказуються у вигляді ініціалів.

3. Нормативні посилання

ISO 9001:2008 Системи управління якістю. вимоги;

ISO/IEC 27001:2013 Системи менеджменту інформаційної безпеки.

4. Загальні положення

4.1. Під інформаційною безпекою розуміється стан захищеності інформації, що характеризується здатністю персоналу, технічних засобів і інформаційних технологій забезпечувати конфіденційність, цілісність і доступність інформації при її обробці технічними засобами.

4.2. Політика інформаційної безпеки розроблена відповідно до положень міжнародного стандарту ISO/IEC 27001:2013.

4.3. Політика інформаційної безпеки затверджується Головою ради директорів підприємства Softline.

4.4 Перегляд Політики проводиться на регулярній основі не рідше одного разу на рік.

4.5. Відповідальність за загальний контроль вмісту справжнього документа і внесення в нього змін покладається на Керівника Департаменту безпеки.

5. Цілі в області інформаційної безпеки

В області інформаційної безпеки підприємства Softline встановлюються такі стратегічні цілі:

5.1. Підвищення конкурентоспроможності бізнесу підприємства Softline;

5.2. Відповідність вимогам законодавства і договірних зобов'язаннями в частині інформаційної безпеки;

5.3. Підвищення ділової репутації та корпоративної культури підприємства Softline;

5.4. Ефективне управління інформаційною безпекою та безперервне вдосконалення системи управління інформаційною безпекою;

5.5. Досягнення адекватності заходів щодо захисту від загроз інформаційної

безпеки;

5.6. Забезпечення безпеки корпоративних активів підприємства Softline, включаючи персонал, матеріально-технічні цінності, інформаційні ресурси, бізнес-процеси.

6. Завдання забезпечення інформаційної безпеки

Система забезпечення інформаційної безпеки підприємства Softline має вирішувати такі завдання:

6.1. Залучення вищого керівництва підприємства Softline до процесу забезпечення інформаційної безпеки: діяльність по забезпеченню

інформаційної безпеки ініційована і контролюється вищим керівництвом підприємства Softline;

6.2. Відповідність вимогам законодавства РФ: підприємство Softline реалізує заходи забезпечення інформаційної безпеки відповідно до чинного законодавства і договірних зобов'язань;

6.3. Узгодженість дій щодо забезпечення інформаційної, фізичної та економічної безпеки: дії щодо забезпечення інформаційної, фізичної та економічної безпеки здійснюються на основі чіткої взаємодії зацікавлених підрозділів підприємства Softline і узгоджені між собою за цілями, завданнями, принципами, методами і засобами;

6.4. Застосування економічно доцільних заходів: підприємство Softline прагне вибирати заходи забезпечення інформаційної безпеки з урахуванням витрат на їх реалізацію, ймовірності виникнення загроз інформаційної безпеки та обсягу можливих втрат від їх реалізації;

6.5. Перевірка працівників: всі кандидати на вакантні посади в підприємстві Softline в обов'язковому порядку проходять перевірку в відповідно до встановлених процедур;

6.6. Документованість вимог інформаційної безпеки: в підприємстві Softline всі вимоги в області інформаційної безпеки фіксуються в розроблюваних внутрішніх нормативних документах;

6.7. Підвищення обізнаності в питаннях забезпечення інформаційної безпеки: документовані вимоги в області інформаційної безпеки доводяться до відома працівників всіх бізнес-підрозділів підприємства Softline і контрагентів в частині що їх стосується;

6.8. Реагування на інциденти інформаційної безпеки: підприємство Softline прагне виявляти, враховувати і оперативно реагувати на дійсні та ймовірні порушення інформаційної безпеки;

6.9. Оцінка ризиків: в підприємстві Softline на постійній основі реалізуються заходи з оцінки та управління ризиками інформаційної безпеки, підвищенню рівня захищеності інформаційних активів;

6.10. Врахування вимог інформаційної безпеки в проектній діяльності: крім операційної діяльності, підприємство Softline прагне враховувати вимоги інформаційної безпеки в проектній діяльності. Розробка і документування вимог по забезпеченню інформаційної безпеки здійснюється

на початкових етапах реалізації проектів, пов'язаних з обробкою, зберіганням і передачею інформації;

6.11. Постійне вдосконалення системи управління інформаційною безпекою: вдосконалення системи управління інформаційної безпеки є безперервним процесом.

7. Принципи забезпечення інформаційної безпеки

7.1. Принцип системності. У підприємстві Softline активи розглядаються, як взаємопов'язані і взаємовпливаючі компоненти єдиної системи. Враховується максимально можлива кількість сценаріїв поведінки системи в разі виникнення загроз інформаційній безпеці. Система захисту будується з урахуванням не тільки всіх відомих каналів отримання несанкціонованого доступу до інформації, а й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеки;

7.2. Принцип повноти (комплексності). Для забезпечення інформаційної безпеки використовується широкий спектр заходів, методів і засобів захисту інформації. комплексне їх використання передбачає узгодження різнорідних засобів при побудові цілісної системи захисту, що перекривають всі існуючі канали загроз і немістять слабких місць на стиках окремих її компонентів;

7.3. Принцип ешелонування. Не можна покладатися на один захисний рубіж, яким би надійним він не здавався. Система забезпечення інформаційної безпеки будується таким чином, щоб зона безпеки перебувала, яку потрібно захищати найбільше, перебувала всередині інших зон;

7.4. Принцип рівноміцності. Ефективність захисних механізмів не повинна бути зведена нанівець слабкою ланкою, що виникла в результаті недооцінки реальних загроз або застосування неадекватних заходів захисту;

7.5. Принцип безперервності. У підприємстві Softline забезпечення інформаційної безпеки є безперервним цілеспрямованим процесом, який передбачає прийняття відповідних заходів на всіх етапах життєвого циклу активів.

7.6. Принцип розумної достатності. Керівництво підприємства Softline виходить з того, що створити «абсолютний» захист активів неможливо. Тому вибір засобів захисту активів, адекватний реально існуючим загрозам (тобто забезпечується допустимий рівень можливого збитку в разі реалізації загроз), здійснюється на основі проведення аналізу ризиків;

7.7. Принцип законності. При виборі і реалізації заходів і засобів забезпечення інформаційної безпеки підприємство Softline строго дотримується законодавства Російської Федерації, вимог нормативних правових і технічних документів в галузі забезпечення інформаційної безпеки підприємства Softline;

7.8. Принцип керованості. Всі процеси управління і забезпечення інформаційної безпеки в підприємстві Softline повинні бути керованими, тобто повинна бути можливість моніторингу і вимірювання процесів і компонентів, своєчасного виявлення порушень інформаційної безпеки і прийняття відповідних заходів;

7.9. Принцип персональної відповідальності. Відповідальність за забезпечення безпеки активів покладається на кожного працівника в межах його повноважень.

8. Розподіл ролей і відповідальності. Для ефективного впровадження процесів управління інформаційною безпекою в підприємстві Softline впроваджується система управління інформаційною безпекою на основі вимог Міжнародного стандарту ISO / IEC 27001 до: 2013. Система управління інформаційної безпекою регламентується окремими положеннями і стандартами, прийнятими підприємством Softline.

8.1. Підрозділи інформаційної безпеки:

- спільно з представниками бізнес-підрозділів і підрозділів Департаменту інформаційних технологій, включаючи відокремлені підрозділи підприємства, що займаються підтримкою і впровадженням інформаційних сервісів (далі IT), проводять оцінку ризиків, пов'язаних з захистом інформації, і здійснюють управління цими ризиками;

- спільно з підрозділами IT розробляють і впроваджують політики та стандарти інформаційної безпеки, засновані на визнаних в світі стандартах інформаційної безпеки;

- розробляють плани і технічні специфікації для впровадження систем інформаційної безпеки;

- визначають вимоги щодо інформаційної безпеки для існуючих і впроваджуваних інформаційних систем;

- обґрунтовують і спільно з ІТ захищають загальний бюджет ІТ в частині, що стосується інформаційної безпеки підприємства Softline, з метою виділення достатніх коштів для функціонування і розвитку систем інформаційної безпеки;

- беруть участь в розробці стандартів, інструкцій та інших нормативних документів в сфері ІТ, виборі контрагентів та затвердження технічних рішень в частині інформаційної безпеки;

- проводять аудит інформаційних систем з метою виявлення потенційних вразливостей в корпоративних інформаційних системах, використовують надані ІТ можливості і інструменти, організовують оповіщення користувачів про спроби вторгнення в інформаційні системи;

- можуть залучати ресурси сторонніх фірм для проведення аудиту інформаційних систем з точки зору інформаційної безпеки;

- організовують і проводять навчання співробітників підприємства з інформаційної безпеки, перевіряють знання і навички інформаційної безпеки співробітників підприємства;

- беруть активну участь в процесі зміни інформаційних систем для забезпечення необхідного рівня інформаційної безпеки;

- узгоджують і контролюють доступ користувачів до інформаційних ресурсів;

- проводять постійну роботу з користувачами інформаційних ресурсів підприємства з роз'яснення їм основних вимог інформаційної безпеки.

8.2. Підрозділи Інформаційних технологій:

- впроваджують нові інформаційні системи і інструменти, забезпечують реалізацію спільно розроблених політик, стандартів інформаційної безпеки;

- забезпечують працездатність і доступність інформаційних систем;

- сприяють дотриманню всих спільно розроблених вимог інформаційної безпеки;

- розробляють і впроваджують плани розвитку інформаційних систем,

- забезпечують фінансування і здійснюють всі види технічної

- діяльності в корпоративних інформаційних системах;

- слідують спільно прийнятим корпоративним політикам, стандартам і інструкціям з інформаційної безпеки, так само як і своїм функціональними обов'язками;

- слідують спільно розробленим вимогам і рекомендаціям підрозділів інформаційної безпеки на всіх стадіях реалізації нових проектів: від пропозиції і планування до здійснення;
- керують процесом зміни інформаційних систем підприємтва Softline;
- негайно інформують підрозділи інформаційної безпеки про будь-які порушення, вразливості, виявлених в корпоративних інформаційних системах і спробах незаконного проникнення в них;
- забезпечують доступ користувачів до комп'ютерних систем;
- є власником бюджету IT, включаючи статті витрат на інформаційну безпеку, і забезпечують фінансування затверджених проектів інформаційної безпеки;
- забезпечують технічну експлуатацію систем безпеки.

9. Відповідальність за порушення політики інформаційної безпеки

У разі порушення встановлених правил роботи з інформаційними активами працівник може бути обмежений в правах доступу до таких активів, а також притягнутий до відповідальності відповідно до Трудового кодексу, Кодексу про адміністративні правопорушення та Кримінального кодексу РФ.