МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАОЧНОГО ТА ДИСТАНЦІЙНОГО НАВЧАННЯ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

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

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему: **«МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ»**

Студент групи УБЗМ-7 Кавун Андрій Володимирович _____
(підпис)

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

Нормоконтроль: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2020

Державний університет телекомунікацій
Навчально-науковий інститут заочного та дистанційного навчання
Кафедра управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ
на магістерську атестаційну роботу
студенту Кавуну Андрію Володимировичу

1. Тема роботи: «МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ» затверджена наказом ректора від «___» _____ 20__ р. № ___.

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

3. Об’єкт дослідження: система управління інформаційною безпекою підприємства.

4. Предмет дослідження: методичне забезпечення політики інформаційної безпеки на підприємстві.

5. Мета дослідження: надати пропозиції щодо методичного забезпечення політики інформаційної безпеки на підприємстві.

6. Перелік питань, які мають бути розроблені:
1. Теоретичні основи дослідження інформаційної безпеки підприємства.
2. Особливості формування політики інформаційної безпеки на підприємстві.
3. Методика розробки документу «Політика інформаційної безпеки» підприємства.

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

Науковий керівник: Мордас І. В.

Завдання прийнято до виконання: Кавун А. В.

Державний університет телекомунікацій
Навчально-науковий інститут заочного та дистанційного навчання
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської атестаційної роботи
студентом Кавуном Андрієм Володимировичем

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.	11.03.2020	
2.	Збір та аналіз літератури.	18.03.2020	
3.	Написання 1-го розділу роботи.	01.04.2020	
4.	Написання 2-го розділу роботи.	15.04.2020	
5.	Написання 3-го розділу роботи.	29.04.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	06.05.2020	
7.	Оформлення роботи.	12.05.2020	
8.	Оформлення презентації.	14.05.2020	
9.	Отримання рецензії на роботу.	20.05.2020	
10.	Захист в ДЕК.	__.06.2020	

Студент групи УБЗМ-71 Кавун Андрій Володимирович _____
(підпис)

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

Нормоконтроль: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

РЕФЕРАТ

Робота містить вступ, три розділи, висновки, список використаних джерел. Загальний обсяг роботи – 73 сторінки.

Об’єкт дослідження – система управління інформаційною безпекою підприємства.

Предмет дослідження – методичне забезпечення політики інформаційної безпеки на підприємстві.

Мета дослідження – надати пропозиції щодо методичного забезпечення політики інформаційної безпеки на підприємстві.

У роботі визначено теоретичні основи дослідження інформаційної безпеки підприємства. Проаналізовано особливості формування політики інформаційної безпеки на підприємстві. Досліджено методику розробки документу «Політика інформаційної безпеки» підприємства.

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

ЗМІСТ

ВСТУП

Актуальність теми. Розвиток і зміцнення позицій, а також забезпечення ефективного і безперебійного функціонування є цілями діяльності будь-якого підприємства. Найважливішою умовою реалізації цих цілей є забезпечення необхідного і достатнього рівня інформаційної безпеки підприємства, який визначаються рівнем інформаційної безпеки технологічних процесів та автоматизованих систем, що експлуатуються підприємствами.

Особливості функціонування підприємства полягають у тому, що негативні наслідки збоїв у роботі окремих функцій можуть призвести до втрати можливості їх функціонування, завдати шкоди інтересам власників і клієнтів. Тому для підприємства загрози інформаційній безпеці становлять істотну небезпеку. Для протистояння таким загрозам та забезпечення ефективності заходів щодо їх ліквідації на підприємствах необхідно забезпечити достатній рівень інформаційної безпеки. Тому, забезпечення інформаційної безпеки є для підприємства одним з основних аспектів його діяльності.

При цьому, важливим елементом у системі управління інформаційною безпекою підприємства є власне методичне забезпечення політики інформаційної безпеки на підприємстві. Саме тому, важливо здійснити аналіз методики його розробки, що дасть можливість підприємствам використати та адаптувати її до власних особливостей функціонування.

Мета і завдання дослідження. Мета дослідження – надати пропозиції щодо методичного забезпечення політики інформаційної безпеки на підприємстві.

Відповідно до мети передбачено вирішити такі *завдання*:

- визначити теоретичні основи дослідження інформаційної безпеки підприємства;
- проаналізувати особливості формування політики інформаційної безпеки на підприємстві;

– дослідити методику розробки документу «Політика інформаційної безпеки» підприємства.

Об'єктом дослідження є система управління інформаційною безпекою підприємства.

Предметом дослідження є методичне забезпечення політики інформаційної безпеки на підприємстві.

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

Структура роботи. Робота містить вступ, три розділи, висновки, список використаних джерел. Загальний обсяг роботи – 83 сторінки.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Сутність інформаційної безпеки підприємства

Інформаційна безпека підприємства – це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Крім того, під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури.

Інформаційна безпека включає в себе заходи по захисту процесів створення даних, їх введення, обробки і виводу. Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства в цілісності, захист і гарантування повноти і точності інформації, яку вона видає, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Інформаційна безпека – це комплекс заходів, які забезпечує для охоплюваної ним інформації наступні фактори:

- конфіденційність – властивість, яка гарантує, що інформація недоступна і не може бути розкрита несанкціонованими особами, об’єктами чи процесами. Можливість ознайомитись з інформацією мають лише ті особи, які володіють відповідними повноваженнями;
- цілісність – властивість, яка гарантує, що система повноцінно виконує свої функції без навмисних чи випадкових несанкціонованих втручань. Можливість внести зміни в інформацію повинні мати лише ті особи, які на це вповноважені;

- доступність – можливість отримання авторизованого доступу до інформації з боку вповноважених осіб в відповідний санкціонований для роботи період часу.

Виділяють і інші не завжди обов'язкові фактори моделі безпеки:

- неспростовність ─ неможливість відмови від авторства, тобто особа, яка направила інформацію іншій особі, не може відректися від факту відправлення інформації, а особа, яка отримала інформацію, не може відректися від факту її отримання. Забезпечується засобами криптографії (електронно-цифровим підписом);
- властивість, яка гарантує, що ідентифікатори предмета чи ресурсу задовольняють необхідні вимоги. Достовірність застосовують до об’єктів: споживачів, процесів, систем чи інформації;
- підзвітність ─ забезпечення ідентифікації суб'єкта доступу та реєстрації його дій, тобто всі значимі дії особи, які вона виконує в рамках, що контролюються системою безпеки, повинні бути зафіксовані і проаналізовані. Зазвичай облік ведеться засобами електронних реєстраційних журналів, які використовуються в основному лише вповноваженими службами;
- достовірність - властивість відповідності передбаченій поведінці чи результату;
- автентичність ─ властивість, що гарантує, що суб'єкт або ресурс ідентичні заявленим.

Сутність загроз інформаційної безпеки зводиться, як правило, до нанесення того чи іншого збитку підприємству (організації).

Прояви можливого збитку можуть бути найрізноманітнішими:

- моральна і матеріальна шкода діловій репутації організації;
- моральний, фізичний чи матеріальний збиток, пов'язаний з розголошенням персональних даних окремих осіб;
- матеріальний (фінансовий) збиток від розголошення конфіденційної інформації;

- матеріал (фінансовий) збиток від необхідності відновлення порушених інформаційних ресурсів, які захищаються;
- матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов'язань перед третьою стороною;
- моральний і матеріальний збиток від дезорганізації в роботі всього підприємства.

Джерела зовнішніх загроз можуть бути випадковими і запланованими та мати різний рівень кваліфікації. До них відносяться:

- кримінальні структури;
- потенційні злочинці і хакери;
- нечесні партнери;
- технічний персонал постачальників послуг, тощо.

Внутрішні суб'єкти (джерела), як правило, представлені висококваліфікованими фахівцями у галузі розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв'язуваних завдань, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного устаткування і технічних засобів мережі. До них відносяться:

- основний персонал (користувачі, програмісти, розробники);
- представники служби захисту інформації;
- допоміжний персонал (прибиральники, охорона);
- технічний персонал;

Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути зовнішніми:

- засоби зв'язку;
- мережі інженерних комунікації;
- транспорт.

Та внутрішніми:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- допоміжні технічні засоби (охорони, сигналізації, телефонії);
- інші технічні засоби, що застосовуються в установі.

Відповідно, дії, які можуть завдати шкоди інформаційній безпеці організації, можна також розділити на кілька категорій:

- дії, які здійснюються авторизованими користувачами. У цю категорію потрапляють: цілеспрямована крадіжка або знищення даних на робочій станції або сервері; пошкодження даних користувачів у результаті необережних дій;
- «Електронні» методи впливу, які здійснюються хакерами. До таких методів відносяться: несанкціоноване проникнення в комп'ютерні мережі, DOS атаки;
- Комп'ютерні віруси. Окрема категорія електронних методів впливу - комп'ютерні віруси та інші шкідливі програми. Проникнення вірусу на вузли корпоративної мережі може призвести до порушення їх функціонування, втрат робочого часу, втрати даних, викраденні конфіденційної інформації і навіть прямим розкраданням фінансових коштів. Вірусна програма, яка проникла в корпоративну мережу, може надати зловмисникам частковий або повний контроль над діяльністю компанії.
- «Природні» загрози. На інформаційну безпеку компанії можуть впливати різноманітні зовнішні фактори. Так причиною втрати даних може стати неправильне зберігання, крадіжка комп'ютерів і носіїв, форс-мажорні обставини і т.д.

У сучасних умовах наявність розвиненої системи інформаційної безпеки стає однією з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якої компанії.

Отже, бурхливий розвиток інформаційних технологій призвів до інформаційної революції, внаслідок чого основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці національної безпеки.

З одного боку, використання інформаційних технологій дає ряд очевидних переваг: підвищення ефективності процесів управління, обробки і передачі даних і т.п. У наш час вже неможливо уявити велику організацію без застосування новітніх інформаційних технологій, починаючи від автоматизації окремих робочих місць і закінчуючи побудовою корпоративних розподілених інформаційних систем.

З іншого боку, розвиток мереж, їх ускладнення, взаємна інтеграція, відкритість призводять до появи якісно нових загроз, збільшенню числа зловмисників, які мають потенційну можливість впливати на систему.

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

З урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства необхідно передбачити перехід від принципу гарантування безпеки інформації до принципу інформаційної безпеки.

1.2. Політика інформаційної безпеки на підприємстві

Вимоги стандартів для роботи бізнесу, як правило, надлишкові. Виходячи з досвіду, компанія Brainkeeper виділяє наступні ключові ризики сучасного бізнесу:

- втрата даних організації: втрата даних через збій обладнання, втрата даних через людський фактор (несанкціоноване знищення інформації користувачем, втрата або вилучення носіїв інформації);
- тимчасова недоступність сервісів, простій в роботі: неможливість працювати через збій мережі і систем, вірусні епідемії, мережеві атаки, вразливості програмного забезпечення;
- витік інформації: можливість винесення інформації співробітниками компанії (особливо при звільненні), можливість співробітника переглядати і копіювати всі файли організації;
- втрата робочого часу співробітників: використання робочого часу та інтернету в особистих цілях (соціальні мережі, он-лайн ігри, icq, skype)

Дане завдання вже не нове, і ефективні рішення для підприємства можна застосувати без тривалого вивчення міжнародних стандартів безпеки. Вирішити проблеми інформаційної безпеки компанії можна, звернувшись до допомоги кваліфікованих фахівців. Витрати на проведення робіт при цьому будуть значно нижчими, ніж час, витрачений на вивчення документів і технічних засобів, підготовку необхідних політик, економічних обґрунтувань.

Запропонована методика розробки політики інформаційної безпеки (ІБ) підприємства дозволяє повністю проаналізувати і документально оформити вимоги бізнесу до цих процесів. Економічна оцінка обґрунтувань технічних та організаційних заходів захисту дозволяє уникнути витрат на зайві заходи безпеки, можливі при суб'єктивній оцінці ризиків, а також надати допомогу в плануванні та здійсненні захисту на всіх стадіях бізнес процесів.

Головна мета будь-якої системи ІБ полягає у забезпеченні сталого функціонування об'єкта в розрізі критеріїв оцінки:

- конфіденційність - інформація повинна бути доступна тільки тим, хто з нею повинен працювати;
- цілісність - інформація повинна змінюватися тільки легітимними методами;
- доступність - інформація повинна бути доступна на всіх етапах технологічних процесів для успішної роботи бізнесу;
- спостерігаємість - будь-які зміни інформації не повинні відбуватися безслідно.

Для досягнення цих цілей з деталізацією, необхідною і достатньою для бізнесу, проводиться аудит безпеки на підприємстві. В результаті аудиту керівництво підприємства отримує об'єктивну картину стану справ ІБ та рекомендації щодо застосування кращих практик міжнародних стандартів. Такі рекомендації можуть містити оновлення політик безпеки, або ж обґрунтування для їх створення. Типові політики безпеки для сучасного підприємства:

- положення про безпеку на підприємстві;
- політика антивірусного захисту;
- політика ПК (стандартизація програмного забезпечення та налаштувань операційних систем)
- політика призначення прав користувачу
- керівництво з фізичної безпеки (регламентований доступ до приміщень, плани евакуації, журнали обліку відкриття приміщень, інструкція для персоналу, пожежна безпека)

Якщо обмежити дії користувачів лише адміністративно без технічної реалізації, то така політика буде наносити більше шкоди, ніж користі. Вирішенням можуть послужити:

- антивірусне ПЗ;

- керування користувачами (Active Directory);
- міжмережеві екрани
- системи контролю доступу до приміщень

Важливо розуміти, що перед впровадженням будь-яких технічних або організаційних заходів щодо захисту інформації, необхідно розробити політики безпеки, адекватні цілям і завданням бізнесу підприємства. Наприклад, одна з політик безпеки повинна описувати порядок надання та використання прав користувачів, а також вимоги відповідальності користувачів за свої дії на підприємстві. Система ІБ буде ефективною, якщо політики, що визначають вимоги, засоби, що реалізують політики, і бізнес завдання підприємства гармонійно доповнюють один одного в досягненні спільних цілей.

Отже, в інтересах будь-якого керівника створити ефективні політики безпеки на підприємстві. Коли в компанії немає формалізованих правил і контролю дисципліни, це викликає певні проблеми, пов'язані з ефективністю як окремо взятого співробітника, так і організації в цілому. Темпи розвитку бізнесу та технологій часто значно випереджають темпи розробки нормативно-правової бази. Навіть якщо відбуваються зміни в документах, залишається проблема доведення їх до відома користувачів та контролю рівня знань.

Така ситуація призводить до необхідності, крім законів України та інших нормативних документів в цій галузі, використовувати ряд міжнародних рекомендацій. У тому числі адаптувати їх до конкретного підприємства і застосовувати на практиці методики міжнародних стандартів, таких як: ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL і інші. Завдання використання методик управління інформаційними ризиками в сукупності з оцінками економічної ефективності інвестицій для забезпечення захисту інформації підприємства значно ускладнюється, враховуючи специфічні вимоги бізнесу.

1.3. Документ «Політика інформаційної безпеки» в системі забезпечення інформаційної безпеки підприємства

Основою заходів по забезпеченню режиму інформаційної безпеки адміністративного рівня, тобто заходів, що робляться керівництвом організації, є розробка документу «Політика інформаційної безпеки» підприємства. Під політикою безпеки розуміється сукупність документованих управлінських рішень, направлених на захист інформації і асоційованих з нею ресурсів. Документ «Політика інформаційної безпеки» підприємства визначає основні напрями і вимоги по забезпеченню інформаційної безпеки підприємства. Положення документу відносяться до всього штатного персоналу, тимчасових службовців і інших співробітників підприємства, а також клієнтів підприємства і третіх осіб, що мають доступ до автоматизованих і телекомунікаційних систем підприємства. Приклад такого документу наведено у Додатку А.

Забезпечення безпеки інформації включає будь-яку діяльність, направлену на захист інформації і/або підтримуючої інфраструктури. Справжня політика інформаційної безпеки охоплює всі автоматизовані і телекомунікаційні системи, власником і користувачем яких є Підприємство.

Не існує єдиної оптимальної структури захисту інформації. Кожна категорія користувачів або фахівців з інформаційних технологій, що працюють в конкретному середовищі, може мати свій власний, такий, що відрізняється від інших, набір вимог, проблем і пріоритетів, залежно від функцій конкретної організації і виробничого або обчислювального середовища.

Багато організацій вирішують цю проблему, розробляючи набір окремих керівних принципів для відповідних груп співробітників, щоб забезпечити ефективніше розповсюдження знань в області захисту інформації. Організаціям, що вирішили прийняти іншу структуру (або навіть розробити свої рекомендації), бажано ввести перехресні посилання на текст діючих правил, щоб їх майбутні ділові партнери або аудитори могли встановити прямі

зв'язки між цим стандартом і прийнятими в даній організації принципами системи захисту інформації.

Метою політики інформаційної безпеки є забезпечення підтримки інформаційної безпеки керівництвом організації.

Вище керівництво повинне поставити чітку мету і всесторонньо подавати свою підтримку інформаційної безпеки за допомогою розповсюдження політики безпеки серед співробітників організації.

Письмовий документ про політику безпеки повинен бути доступний всім співробітникам, що відповідають за забезпечення інформаційної безпеки.

Головною причиною появи політики безпеки є вимога наявності такого документа від регулятора – організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності. Крім того, певні вимоги (рекомендації) пред’являють галузеві або загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається у вигляді зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства. Відсутність політики викликає негативну оцінку, яка в свою чергу впливає на публічні показники підприємства – позиції в рейтингу, рівень надійності і т.д. Цікаво, що, згідно з дослідженням з безпеки, проведеного компанією Deloitte в 2006 році, підприємства, які мають формалізовані політики інформаційної безпеки, значно рідше піддаються злому. Це свідчить про те, що наявність політики є ознакою зрілості підприємства в питаннях інформаційної безпеки. Те, що підприємство виразно сформулювало свої принципи і підходи до забезпечення інформаційної безпеки означає, що в цьому напрямку була проведена серйозна робота.

Темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендаційної та нормативно-правової бази керівних документів. Тому вирішення питання про розробку ефективної політики інформаційної безпеки на сучасному підприємстві обов’язково

пов’язане з проблемою вибору критеріїв і показників захисту, а також ефективності корпоративної системи захисту інформації.

Внаслідок цього, в доповнення до вимог і рекомендацій стандартів, вітчизняного законодавства доводиться використовувати ряд міжнародних рекомендацій. В тому числі адаптувати до вітчизняних умов и застосовувати на практиці методики міжнародних стандартів, таких, як ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL та інші, а також використовувати методики управління інформаційними рисками в сукупності з оцінками економічної ефективності інвестицій в забезпечення захисту інформації підприємства.

Отже, забезпечення інформаційної безпеки є необхідною умовою для здійснення діяльності підприємства. Порушення інформаційної безпеки може привести до серйозних наслідків, включаючи втрату довіри з боку клієнтів і зниження конкурентоспроможності.

Висновки до розділу 1

Під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури.

Політика інформаційної безпеки підприємства включає набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Політика інформаційної безпеки може бути викладена як на описовому рівні, так і за допомогою певної формальної мови. системи. Формальний вираз політики інформаційної безпеки називають моделлю політики інформаційної безпеки. Основна мета створення політики інформаційної безпеки й опису її у вигляді формальної моделі ─ це визначення умов, яким має підпорядковуватися поведінка підприємства, вироблення критерію безпеки і проведення формального доведення відповідності підприємства цьому критерію при додержанні встановлених правил і обмежень.

РОЗДІЛ 2.
ОСОБЛИВОСТІ ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

2.1. Розробка політики інформаційної безпеки підприємства

Настання будь-якої з кризових ситуацій може бути спричинене неправомірним використанням інформаційних активів організації, а результатом стає ризик втрати бізнесу. Безумовно, кризові ситуації можуть настати і внаслідок форс-мажорних ситуацій, але - як показує практика і статистика - загрози в області інформаційної безпеки істотно більш реальні.

Залежність фінансових організацій від комп'ютерних і телекомунікаційних ресурсів свідчить про необхідність розробки планів аварійного відновлення всіх систем у разі виникнення кризової ситуації.

Рекомендується, щоб положення документів щодо забезпечення ІБ організації:

- носили не рекомендаційний, а обов'язковий характер;
- були здійсненними і контрольованими. Не рекомендується включати до складу цих документів положення, контроль реалізації яких важкий або неможливий;
- були адекватні вимогам та умовам ведення діяльності (включаючи загрози і ризики ІБ), у тому числі в умовах їх мінливості;
- не суперечили один одному.

В склад документів організації рекомендується включити документ (класифікатор), що містить перелік і призначення всіх документів організації , що регламентують діяльність щодо забезпечення ІБ організації. Зазначений класифікатор може бути корисний при здійсненні менеджменту документів організації, для підвищення ступеня поінформованості працівників організації, а також при виконанні аудиту інформаційної безпеки організації.

При наявності у організації мережі філій (територіальних установ) у кожна з філій рекомендується мати єдиний для організації, затверджений комплект документів щодо забезпечення ІБ. У разі виникнення необхідності врахування специфіки конкретних філій в них повинні бути розроблені власні документи, що враховують цю специфіку. Рекомендується, щоб документи щодо забезпечення ІБ філії організації базувалися на положеннях документів щодо забезпечення ІБ, прийнятих головною організацією і не суперечили їм.

До складу внутрішніх документів організації щодо забезпечення ІБ рекомендується включати наступні види документів (документованої інформації):

- документи, що містять положення корпоративної політики ІБ організації (документи першого рівня), визначають високорівневі цілі, зміст і основні напрямки діяльності по забезпечення ІБ, призначені для організації в цілому;
- документи, що містять положення приватних політик (документи другого рівня), що деталізують положення корпоративної політики ІБ стосовно до однієї або декількох областей ІБ, видів і технологій діяльності організації;
- документи, що містять положення ІБ, що застосовуються до процедур (порядку виконання дій або операцій) забезпечення ІБ (документи третього рівня), містять правила і параметри, які визначають спосіб здійснення і виконання конкретних дій, пов'язаних з ІБ, в рамках технологічних процесів, використовуються в організації, або обмеження щодо виконання окремих дій, пов'язаних з реалізацією захисних заходів, що використовуються в технологічних процесах (технічні завдання, регламенти, порядки, інструкції);
- документи, що містять свідчення виконаної діяльності щодо забезпечення ІБ (документи четвертого рівня), відображають досягнуті результати (проміжні та кінцеві), що відносяться до забезпечення ІБ організації.

Політика має визначати основні ролі, норми і принципи інформаційної безпеки компанії і бути обов'язковою для співробітників компанії та партнерів.

2.2. Загрози політиці інформаційної безпеки на підприємстві

Інформаційна безпека (ІБ) – захист інформації та підтримка інформаційної інфраструктури від випадкового і навмисного впливу природного або штучного характеру, що впливає на власників і користувачів інформації, інфраструктуру в цілому. Процес захисту інформації являє собою взаємодію загроз інформації та інформаційної безпеки, що перешкоджає їхній взаємодії.

Захист інформації відбувається поетапно і у свідомо певному порядку. Кожен з етапів може бути представлений власною моделлю (рис. 2.1).

Рис. 2.1. Модель розподіленого використання ресурсів для захисту інформації

Всі етапи об'єднуються в цілісну модель розподілу ресурсів для захисту інформації. Вона заснована на можливостях ворога і сторони, що захищається, на базі моделі загроз і моделі оцінки втрат. Це відбувається тому, що вартість захисту не повинна перевищувати шкоду порушення безпеки [44].

В даний час існує світова практика забезпечення режиму інформаційної безпеки. На думку Петренка С.А. [10], незалежно від розміру підприємства та

специфіки зусиль, спрямованих на забезпечення режиму ІБ, зазвичай в нього входять етапи, представлені на рис. 2.2.

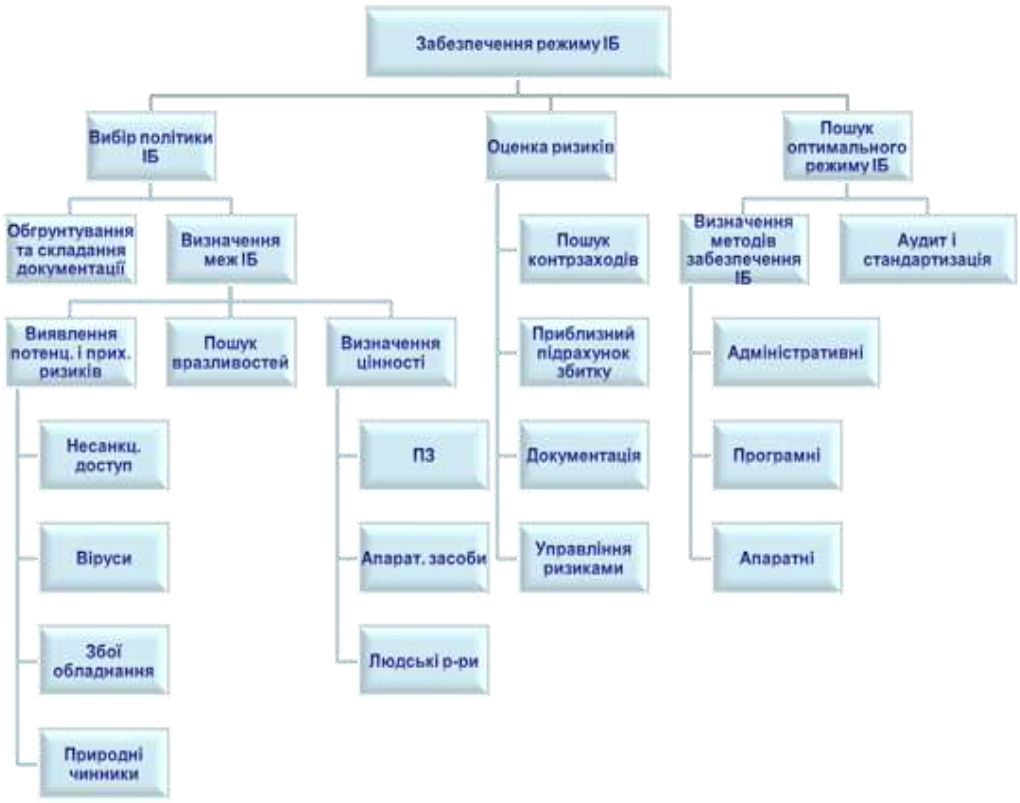

Рис. 2.2. Схема забезпечення режиму інформаційної безпеки

Мінімальна кількість вимог для інформаційної безпеки відповідає основному рівню забезпечення ІБ. Такі вимоги зазвичай застосовуються для стандартних проектів. Якщо базових вимог недостатньо, можна і потрібно застосовувати додаткові, більш високі вимоги. Для цього, крім обліку стандартного списку загроз, обов'язково слід визначити вартість ресурсу, порахувати можливість виникнення загрози, проаналізувати уразливість ресурсу і порахувати потенційний збиток. За результатами вищезазначеного, в табл. 2.1 проведено аналіз режимів інформаційної безпеки.

Набір мінімальних вимог до режиму інформаційної безпеки, перерахованих в стандартах ISO 17799 (міжнародний стандарт), BSI (Німеччина), NIST 800–30 (США), складає основу інформаційної безпеки. Цього набору достатньо для цілого ряду стандартних проектів малого бізнесу. У його рамках можна використовувати особливі стандарти і специфікації, які

мають мінімальний перелік найбільш ймовірних загроз, таких як віруси, несанкціонований доступ, та інші.

Таблиця 2.1

Аналіз режимів інформіційної безпеки

Критерії	Базовий рівень безпеки	Рівень безпеки з підвищеними вимогами
Вимоги	Мінімальні	Ретельна перевірка інформаційного ресурсу на цілісність, доступність, конфіденційність
Вибір методики захисту	Стандартні способи захисту коригуються під дану інформаційну систему	Вибір засобів захисту, що підходять саме до цієї системі. Нестандартні рішення для максимальної безпеки
Вирішальний фактор для вибору режиму ІБ	Вартість	Ефективність

Для виконання більш специфічних вимог до безпеки необхідно розробляти індивідуальний, підвищений режим безпеки [30]. Цей режим передбачає стратегії роботи з ризиками різних класів, в яких реалізуються такі підходи:

- зниження ризиків: багато ризики можуть бути знижені за рахунок використання простих і дешевих контрзаходів;
- неприйняття ризику: деякі класи ризику можна уникнути за допомогою виведення веб–сервера організації за межі локальної мережі;
- зміна характеру ризику: якщо неможливо ухилитися від ризику або зменшити його, то краще застрахувати вразливий об'єкт;
- прийняття ризику: фахівець повинен знати залишкову цінність ризику через неможливість зведення його до малої величині.

В результаті, беручи до уваги всі перераховані вище моменти, можливо створити досить ефективну систему ризик–менеджменту для підприємства.

Сьогодні, серед пріоритетів малих підприємств, ризик–менеджмент знаходиться в самому кінці їхнього списку. Опитування, що проводилося на Американському бізнес–саміті в травні 2010 року показав наступне розподіл пріоритетів [44]:

- ринок та продаж;
- управління грошовим потоком;
- залучення фінансів;
- залучення і утримання персоналу;
- виявлення і менеджмент страхових ризиків;
- відповідність законодавству;
- захист від ризиків.

Відповідно до звіту про загрози безпеки в інтернеті, проведеному компанією Symantec в 2011 році, число кібер–атак на комп'ютери збільшилося на 36% порівняно з 2010 роком. Щодня відбувається більше 4500 нових атак. Було створено понад 403 мільйонів нових різновидів шкідливого програмного забезпечення – що означає збільшення нових розробок на 41% [44].

Дослідження, проведене 874 сертифікованими професіоналами в галузі інформаційної безпеки (CISSP) у 2004 році, показало, що для поліпшення ситуації в галузі інформаційної безпеки потрібна підтримка топ-менеджменту компанії, який недостатньо обізнаний про важливість питання [29].

Перераховані вище статистичні дані дозволяють судити про те, що корпоративні мережі в даний момент є найбільш схильними атакам. Оскільки вони використовують мережі зберігання даних, зв'язки peer–to–peer, миттєві повідомлення, віддалений доступ, то визначення кордонів безпеки є практично неможливим.

Існує велика кількість програм, для оцінки ризиків безпеки. Наприклад, RA2 art of Risk, vsRisk, RiskWatch, COBRA, РіскМенеджер, і багато інших. З

точки зору використання таких програм у сфері малого бізнесу найкращих результатів з меншими матеріальними витратами можна досягти за допомогою методик OCTAVE–S і CRAMM.

Методи OCTAVE засновані на практичних критеріях OCTAVE, які є стандартними підходами для оцінки ІБ. Дана методика реалізується вручну, без використання програмних засобів. Аналітична команда, що складається з 3-5 осіб, розглядає ризики організаційних активів у їх співвідношенні з цілями бізнесу. Кінцевим результатом методу є організаційно–спрямовану стратегію безпеки і план з пом'якшення наслідків порушень ІБ [36].

На відміну від OCTAVE, CRAMM–CCTA Risk Analysis & Management реалізується за допомогою спеціалізованого програмного забезпечення, яке можна налаштувати для різних галузей. Поточна версія CRAMM 5 відповідає BS 7799 (ISO 17799). Аналіз ризиків за методом CRAMM складається з ідентифікації і розрахунку ризиків на основі оцінок певних ресурсів, вразливостей, загроз і ресурсів. Управління ризиками за допомогою CRAMM допомагає виявити і вибрати контрзаходи для зниження ризиків підприємств розглянутих структур до прийнятного рівня.

2.3. Моделі політики інформаційної безпеки на підприємстві

Серед моделей ПБ найвідомішими є дискреційна, мандатна та рольова. Перші дві досить давно відомі й детально досліджені, а рольова політика є недавнім досягненням теорії та практики захисту інформації.

Дискреційна політика безпеки. Основою дискреційної політики безпеки (ДПБ) є дискреційне управління доступом (Discretionary Access Control - DAC), яке визначається двома властивостями:

- усі суб'єкти й об'єкти мають бути однозначно ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на основі певних зовнішніх відносно системи правил.

Мандатна політика безпеки. Основу мандатної (повноважної) політики безпеки (МПБ) становить мандатне управління доступом (Mandatory Access Control - MAC), яке передбачає, що:

- всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;
- у системі визначено лінійно упорядкований набір міток секретності;
- кожному об'єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому, ─ його рівень секретності в АС;
- кожному суб'єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС,- максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

Рольова політика безпеки. Рольову політику безпеки (РПБ) (Role Base Access Control - RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Отже, рольова модель є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПБ, і жорсткістю правил контролю доступу, що притаманна МПБ.

Три рівні політики безпеки. З практичної точки зору політику безпеки доцільно розділити на три рівні. До верхнього рівня можна віднести рішення, що торкаються організації в цілому. Вони носять дуже загальний характер і, як правило, виходять від керівництва організації. Наприклад, список подібних рішень може включати в себе:

- формування або перегляд самої комплексної програми забезпечення інформаційної безпеки, призначення відповідальних за реалізацію цієї програми;
- формулювання цілей у сфері інформаційної безпеки та визначення загальних напрямів їх досягнення;

- забезпечення технічної бази для дотримання відповідних законів і правил;
- формулювання управлінських рішень з тих питань реалізації програмної безпеки, які повинні розглядатися на рівні організації в цілому.

На політику верхнього рівня впливають цілі організації в галузі інформаційної безпеки: вони формулюються, як правило в термінах цілісності, доступності та конфіденційності. Якщо організація відповідає за підтримку критично важливих баз даних, то на першому плані може стояти зменшення випадків втрат, пошкоджень або спотворень даних. Для організації, що займається наданням послуг, імовірно, важлива актуальність інформації про ці послуги та їх ціни, а також доступність послуг максимальному числу потенційних покупців. Режимна організація, в першучергу, піклується про захист від несанкціонованого доступу - конфіденційності.

На верхній рівень виноситься управління ресурсами захисту та координація їх використання, виділення спеціального персоналу для захисту особливо важливих систем, підтримка контактів з іншими організаціями, що забезпечують чи контролюють режим безпеки.

Сфера політики верхнього рівня повинна бути чітко окреслена. Можливо, це будуть комп'ютерні системи самої організації, а, можливо, і деякі аспекти використання домашніх комп'ютерів у співробітників цієї організації. Можна уявити собі, і таку ситуацію, коли в сферу впливу включаються лише окремі найбільш важливі системи політики інформаційної безпеки підприємства. Вироблення програми інформаційної безпеки верхнього рівня і її здійснення - це завдання певних посадових осіб, за виконання якої вони повинні регулярно звітувати.

Нарешті, політика інформаційної безпеки верхнього рівня, очевидно, повинна вписуватися в існуючі закони держави, а щоб бути впевненими в тому, що їй точно й акуратно слідує персонал підприємства, доцільно розробити систему відповідних заохочень і покарань. А взагалі-то кажучи, на верхній

рівень слід виносити мінімум питань. До середнього рівня можна віднести окремі аспекти інформаційної безпеки, проте важливі для різних систем, експлуатованих організацією.

Політика середнього рівня по кожному подібному аспекту передбачає вироблення відповідного документованого управлінського рішення, в якому зазвичай є:

- опис аспекта. Наприклад, якщо взяти застосування користувачами неофіційного програмного забезпечення, то про нього обов'язково має бути сказано, що це таке забезпечення, яке не було схвалено і / або закуплено на рівні організації;
- вказівка на область її застосування (розповсюдження тієї чи іншої політики інформаційної безпеки). Іншими словами має бути сертифіковано, де, коли, як, по відношенню до кого і чого застосовується дана політика безпеки;
- чіткий розподіл відповідних ролей та обов'язків. У «політичний» документ необхідно включити інформацію про посадових осіб, відповідальних за проведення політики безпеки в життя. Наприклад, якщо для використання працівником неофіційного програмного забезпечення потрібно офіційний дозвіл, то має бути відомо, у кого і як його слід отримувати. Якщо повинні перевірятися диски, принесені з інших комп'ютерів, необхідно описати процедуру перевірки. Якщо неофіційне програмне забезпечення використовувати не можна, слід знати, хто стежить за виконанням цього правила;
- механізм забезпечення «законослухняності». Політика має містити загальний опис заборонених дій і покарання за них;
- вказівки на необхідні «точки контакту». Повинно бути точно відомо, куди слід звертатися за роз'ясненнями, допомогою та додатковою інформацією. Зазвичай «точкою контакту» служить посадова особа.

Політика безпеки нижнього рівня відноситься до конкретних сервісів. Вона включає в себе всього два аспекти - мети і правила їх досягнення, тому її

часом важко відокремити від питань реалізації (надання послуг з інформаційного забезпечення). На відміну від двох верхніх рівнів, розглянута політика нерідко буває набагато більш детальною. Є багато питань, специфічних для окремих сервісів, які не можна єдиним чином регламентувати в рамках всієї організації. У той же час ці питання настільки важливі для забезпечення режиму безпеки, що рішення, які належать до них, повинні прийматися на управлінському, а не технічному рівні. Ось лише кілька прикладів-запитань, на які слід дати відповідь при розробці політики безпеки нижнього рівня:

- хто має право доступу до об'єктів, що підтримуються сервісом?
- за яких умов можна читати і модифікувати дані?
- як організований вилучений доступ до сервісу?

При формулюванні цілей, політика нижнього рівня може виходити з міркувань цілісності, доступності та конфіденційності, але вона не повинна на цьому зупинятися. Її цілі мають бути конкретнішими. Наприклад, якщо мова йде про систему розрахунку зарплати, можна поставити мету, щоб тільки працівникам відділу кадрів і бухгалтерії дозволялося вводити і змінювати інформацію. У більш загальному випадку цілі повинні пов'язувати між собою об'єкти сервісу та логічні з точки зору інформаційної безпеки, осмислені, дії з ними. З цілей зазвичай виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим детальніше правила, чим більш формально вони викладені, тим простіше підтримувати їх виконання програмно-технічними заходами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів, і, ймовірно, їх доведеться часто переглядати.

Керівництву необхідно знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а працівники не виявляться надмірно сковані.

Висновки до розділу 2

Метою розробки політики інформаційної безпеки на підприємстві є забезпечення підтримки інформаційної безпеки його керівництвом, яке повинно поставити чітку мету і всесторонньо подавати свою підтримку інформаційної безпеки за допомогою розповсюдження політики безпеки серед співробітників підприємства.

Процес захисту інформації являє собою взаємодію загроз інформації та інформаційної безпеки, що перешкоджає їхній взаємодії. Захист інформації відбувається поетапно і у свідомо певному порядку. Всі етапи об'єднуються в цілісну модель розподілу ресурсів для захисту інформації. Вона заснована на можливостях зловмисника і сторони, що захищається, на базі моделі загроз і моделі оцінки втрат. Це відбувається тому, що вартість захисту не повинна перевищувати шкоду порушення безпеки.

Основними моделями політики інформаційної безпеки є дискреційна, мандатна та рольова.

РОЗДІЛ 3.
ПРОПОЗИЦІЇ ЩОДО РОЗРОБКИ ДОКУМЕНТУ «ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ» ПІДПРИЄМСТВА

3.1. Пропозиції щодо створення документу «Політика інформаційної безпеки» на підприємстві

Управління інформаційною безпекою в компанії має здійснюватися централізовано. Інформаційна безпека для всіх позицій в організації має підтримуватись менеджером з інформаційної безпеки, який відповідає за процес управління інформаційною безпекою організації. Роль менеджера включає:

- управління інформаційною безпекою в компанії;
- виявлення і аналіз інформаційних ризиків, розробка заходів по зменшенню ризиків інформаційної безпеки та моніторинг;
- розробка правил і принципів інформаційної безпеки, їх реалізація на практиці, контроль над їх дотриманням;
- управління, планування та координація діяльності щодо забезпечення інформаційної безпеки в компанії;
- надання консультацій, підтримка відповідальних за забезпечення інформаційної безпеки Департаментів при плануванні і управлінні проектами або інших заходів;
- розробка і управління програмами навчання персоналу в області інформаційної безпеки.

Кожен співробітник може звернутися безпосередньо до менеджера з інформаційної безпеки з питань інформаційної безпеки.

Інформаційна безпека в організації регулюється наступними документами:

- керівництво: інструкція з інформаційної безпеки;

- політика інформаційної безпеки (цей документ);
- керівництво по захисту персональних даних;
- інші процедури і керівництва з інформаційної безпеки.

Кожен співробітник повинен бути ознайомлений з усіма застосовними документами (стандартами) та дотримуватися їх.

Для співробітників має бути розроблена програма підвищення обізнаності про ризики, загрози та заходи захисту інформації. В рамках цієї програми:

- кожен новий працівник у перший день початку роботи в компанії знайомиться з документом, де викладаються основні правила при роботі з інформацією та інформаційними ресурсами;
- кожен співробітник бере участь у тренінгу з інформаційної безпеки. Це навчання проходить в максимально оперативні терміни після прийому на роботу та повторно проходить один раз на рік у форматі комунікацій електронною поштою і презентацій;

Кожен співробітник (у тому числі керівні посади) зобов'язаний брати участь у тренінгах, проводити самостійне ознайомлення з матеріалами щодо підвищення обізнаності в області інформаційної безпеки.

Інформація повинна бути захищена належним чином відповідно до її чутливості, цінності і рівню важливості для компанії. Для досягнення цієї мети необхідний процес класифікації інформації. Для цілей можна визначити визначені наступні рівні конфіденційності інформації:

- загальнодоступний (найнижчий рівень конфіденційності);
- внутрішній;
- конфіденційний;
- секретний (найвищий рівень конфіденційності).

Далі містяться базові поняття про класифікацію інформації, визначено рівні ступеня захисту інформаційних ресурсів залежно від їх критичності, рівня конфіденційності, цінності або вимог законодавства. Застосування відповідного

рівня захисту інформації в залежності від її класу - відповідальність кожного співробітника.

В документах в електронному вигляді (DOC, PPT, XLS, PDF тощо) класифікація вказується в заголовках, колонтитулах підкладці або документа, при цьому використовуються позначення «Загальнодоступний», «Внутрішній», «Конфіденційний» або «Секретний». Вказане маркування повинне бути позначене на кожному аркуші. Для електронних носіїв інформації, таких як CD/DVD, клас інформації визначається найбільшим рівнем конфіденційності інформації, що міститься на носії.

Загальнодоступний клас - відкрита інформація, пов'язана з організацією, доступна для широкої громадськості. Приклад - інформація, опублікована на корпоративному сайті, в газетних статтях чи друкованих матеріалах, таких, як щорічні звіти, описи продукту і т. п. Маркування носія - «Загальнодоступний» або без маркера, якщо з контексту вмісту очевидно, що інформація відноситься до класу «Загальнодоступний». Базові правила для інформації класу «Загальнодоступний»:

- інформація класифікується як «Загальнодоступний» уповноваженим співробітником Департаменту маркетингу і комунікацій після відповідної перевірки та аналізу.
- при публікації інформації, повинні використовуватися формати які виключають можливість зміни вмісту (PDF, PS), формати, які дозволяють вносити зміни в документ повинні використовуватися тільки при необхідності (DOC, XLS);
- для забезпечення достовірності інформації публікується у відкритих джерелах повинен проводитися моніторинг 4 рази в місяць. У випадку порушень має запускатися відпрацьований механізм реакції зі сторони компанії.

Внутрішній клас - інформація, призначена для використання всередині організації. Даний клас інформації не призначений для використання поза

компанією. Приклад - телефонний довідник, інформація на внутрішньому корпоративному Інтранет сайті. Маркування носія - «Внутрішній» або без маркера - за замовчуванням, інформація без маркера повинна розглядатися як «Внутрішній», крім тих випадків, коли з контексту ясно, що це «Загальнодоступний» клас інформації. Базові правила для інформації класу «Внутрішній»:

- створення і поширення інформації відбувається всередині компанії. Існує точна відповідність між змістом документів і службовими обов'язками співробітників, що мають до них доступ;
- інформація, носії, документи, в яких більше немає необхідності повинні бути коректно утилізовані - з використанням «шредера», видалення файлів даних, форматування жорстких дисків, утилізація носіїв інформації (наприклад CD, DVD).

Конфіденційний клас - інформація, розкриття доступу до якої неуповноваженим особам може призвести до фінансових втрат компанії, привести до порушення законодавства, завдати шкоди репутації або будь-якої іншої шкоди компанії. Приклад - інформація про клієнтів, персональні дані співробітників і третіх осіб, партнерів, інформація про підготовлюваня до випуску продуктів, результати маркетингових досліджень, корпоративні «ноу-хау», інформація, що відноситься до банківської, комерційної таємниці або таємниці страхування. Маркування носія - «Конфіденційний». Базові правила для інформації класу «Конфіденційний»:

- інформація може бути розкрита лише обмеженій групі людей за принципом «необхідно знати», тобто безпосередньо пов'язаним з їх посадовими інструкціями або обов'язками;
- конфіденційну інформацію, не дозволяється виносити за межі організації в будь-якій формі без згоди відповідного керівника організації і власника даних. В випадках, коли така інформація обробляється або передається за межі компанії повинні бути дотримані всі умови для запобігання

витоку або крадіжки даних. Забороняється залишати без нагляду інформацію в будь-якій формі на будь-якому носії (наприклад, в автомобілі, ресторані і т. д..);

- конфіденційна інформація повинна оброблятися, зберігатися і передаватися в згідно з правилами, викладеними в цій Політиці - «Захист чутливої інформації».

Секретний клас - інформація, розкриття доступу не уповноваженим до цієї інформації особам, може призвести до значних фінансових втрат компанії, завдати великої шкоди репутації або будь-якої іншої значної шкоди, або ставить під загрозу існування компанії на ринку. Приклад - стратегічні плани, інформація про майбутні продукти, ключі доступу, паролі до систем і т. д.. Маркування носія - «Секретний» Базові правила для інформації класу «Секретний» такі ж як і для класу «Конфіденційний».

Термін «чутлива інформація» є збірною назвою інформації, класифікованою як «конфіденційна» або «секретна».

Чутлива інформація повинна бути захищена, незалежно від форми, в якій вона існує (файл, друкований документ, копія тощо), протягом усього періоду її існування.

Для забезпечення ефективного захисту інформації, ефективних і гнучких бізнес-процесів важлива персональна відповідальність співробітників за дотримання правил захисту інформації.

Всі співробітники компанії повинні дотримуватися наступних зобов'язань щодо чутливої інформації:

- при будь-якій формі електронного обміну інформацією за межами організації, наприклад, при відправці електронною поштою, роботі в Інтернеті або збереження на USB/CD/DVD, необхідно захищати чутливу інформацію, перш ніж проводити передачу даних. У наведених вище прикладах необхідно використовувати архіватор з установкою пароля на архів. При створення архіву перейдіть в закладку «Додатково» і виберіть «Встановити пароль». Після

відправки архіву електронною поштою надішліть пароль за допомогою смс одержувачу;

- перед початком роботи з чутливою інформацією необхідно пересвідчитися в безпеці вашого оточення, - у відсутності сторонніх осіб, які можуть бачити інформацію на дисплеї і що немає можливості зафіксувати і повторити ваші дії з метою отримання доступу до даних;
- не залишати надруковані документи, дані чи інші форми зберігання інформації у вільному доступі на робочому місці, перед тим як покинути робоче місце переконається, що будь-які носії чутливої інформації знаходяться в недоступному місці під замком, дотримуватися політики «чистого робочого столу»;
- для обговорення питань, що зачіпають чутливу інформацію, вибирати такі місця та оточення, де бесіду буде важко підслухати;
- не залишати повідомлення з чутливою інформацією голосовою поштою;
- при передачі інформації (незалежно від способу) відправник є відповідальним за наступне:

1) знати клас, до якого відноситься інформація, що передається;

2) перевірити достовірність даних про одержувача і його право на отримання даної інформації;

3) забезпечити, щоб ця інформація була недоступна стороннім особам;

- слідкувати за актами соціальної інженерії і не надавати конфіденційну інформацію особам, чия особистість не підтверджена як та, яка має право доступу до запитуваної інформації або якщо є сумніви на цей рахунок;
- доступ третіх осіб до конфіденційної або секретної інформації компанії можливий тільки після того, як буде підписана і набуде чинності угода про нерозголошення, а також будуть встановлені технічні/організаційні заходи щодо захисту такої інформації;

- перенесення інформації для подальшої її обробки (наприклад для завершення роботи на особистому комп'ютері у вихідний і т. д.), на комп'ютер, некерований компанією з використанням USB-носіїв, особистої поштової скриньки або будь-яким іншим способом не дозволяється.

Інформація, що належить компанії, може оброблятися і зберігатися тільки на пристроях, що належать організації.

Знищення даних та утилізація носіїв інформації.

- дані з носіїв інформації, таких як CD/DVD-диски, USB-накопичувачі, а також паперові документи, що містять чутливу інформацію, в яких більше немає необхідності, повинні утилізуватися відповідно - цифрові носії даних з використанням спеціального програмного забезпечення, носії в паперовому вигляді – за допомогою пристроїв знищення документів, так званих «шредерів»;
- знищення інформації або носіїв інформації класифікованих як «секретний» повинно проводитись у відповідності з певними правилами. Процедури повинні відповідати внутрішнім стандартам і нормативним документам у відповідності з вимогами про терміни зберігання даної інформації.
- суворо забороняється викидати документи та носії інформації без попереднього знищення даних на них (навіть якщо інформація була видалена користувачем з носія). У разі необхідності утилізації медіа носіїв необхідно звернутися до менеджера з безпеки для проведення процедури очищення диска за допомогою спеціалізованого ПЗ.

Співробітники, а також треті сторони, зобов'язані зберігати конфіденційність персональних даних, дотримуючись заходів безпеки. До персональних даних належать дані про співробітників, клієнтів, партнерів, агентів, постачальників послуг, інших контр-агентів компанії, а також всі ті дані, які інтерпретуються як «персональні дані» відповідно до Закону України «Про захист персональних даних» №2297-17 від 1 червня 2010 року.

Недотримання правил поводження з даними може поставити під загрозу безпеку персональних даних. Зобов'язання збереження конфіденційності на певний період залишається навіть після припинення трудових відносин або завершення співпраці з організацією. Несанкціоноване надання інформації про персональні дані стороннім особам є грубим порушенням трудової дисципліни і Законодавства України.

Наказ про захист персональних даних визначає вимоги до захисту персональних даних у відповідності з чинним Законодавством.

Доступ в офісні приміщення має контролюватися. Доступ співробітників в офіси здійснюється з використанням іменних карток доступу. Співробітник отримує картку доступу в офіс за відповідною заявою при прийомі на роботу.

Карта доступу використовується для отримання доступу в офісні приміщення, а також з метою реєстрації переміщень працівника в робочий час. При користуванні картками доступу офісних приміщеннях співробітники зобов'язані дотримуватись наступних правил:

- при вході в офіс або переміщенні всередині офісу співробітник повинен реєструватись своєю карткою при наявності реєстратора (турнікети, двері з реєстратором і т. д.);
- працівникам забороняється передавати в користування свої карти доступу іншим особам, співробітникам в тому числі. Співробітникам забороняється надаватись доступ в офіси компанії іншим особам за допомогою своєї картки доступу;
- після входу в приміщення співробітник зобов'язаний переконатися, що двері за ним закриті і ніхто інший не може увійти в приміщення слідом без використання картки доступу;
- працівник зобов'язаний приймати всі можливі заходи для запобігання ушкодження, втрати, крадіжки або неправомірного використання своєї картки доступу в приміщення;

- до працівника можуть бути застосовані дисциплінарні заходи в разі частої (більше двох раз за період 90 днів) втрати картки доступу.

У випадках, коли працівник забуває особисту картку доступу, йому видається тимчасовий пропуск терміном дії на 1 день. Тимчасова картка доступу видається за запитом. Описані вище заходи і правила використання карт доступу відносяться також до ключів в офісні приміщення. Створення копій ключів без погодження уповноважених співробітників забороняється.

Відносно переміщень гостей діють наступні правила (співробітники, які приймають відвідувачів, повинні бути знайомі з зазначеними правилами):

- відвідування офісів третіми особами повинно фіксуватися, співробітник служби охорони повинен бути про це сповіщений.
- гості організації повинні бути зустрінуті приймаючою стороною (співробітником) на «Ресепшн». Після закінчення візиту, приймаюча сторона (працівник) зобов'язана провести гостей до виходу з офісу або на «Ресепшн»;
- у разі необхідності мати доступ в офіс протягом декількох днів представниками партнерів (наприклад, з метою проведення аудиту) може бути видана картка доступу в офіс з обмеженим терміном дії. Контроль за правомірним використанням виданих перепусток третьою стороною несе приймаюча сторона – співробітник, що ініціював видачу даного пропуску. Термін дії перепустки та час роботи тимчасового пропуску повинні бути обмежені в відповідно з необхідністю, але не перевищувати годин нормального бізнес-часу організації. Максимальний термін дії тимчасових карт доступу не повинен перевищувати 60 днів. Перед видачею тимчасового пропуску третій стороні, необхідно ознайомити одержувача з правилами захисту інформації компанії. З компанією, представники якої отримують тимчасовий доступ до офісне приміщення, повинен бути підписаний договір про нерозголошення інформації. Відповідальним за підпис даного документа є Підрозділ, який є відповідальним за взаємодію з третьою стороною або власник проекту, в рамках якого відбувається взаємодія;

- якщо співробітник зустрічає в офісі компанії підозрілу сторонню особу, без супроводження працівника компанії, то він має поцікавитися про мету візиту і провести стороннього на «Ресепшн» або повідомити про цей факт Службу Охорони.

Для мобільних пристроїв (наприклад, ноутбуки, мобільні телефони, КПК тощо) визначені наступні правила:

- за зовнішнім виглядом пристрою не повинно бути зрозуміло, що пристрій належить організації - заборонено використовувати логотип або будь-яку іншу символіку на пристроях, що вказують на належність до компанії;
- ноутбуки, КПК, портативні пристрої повинні бути захищені таким чином, щоб виключити доступ до них сторонніх осіб. Наприклад, за допомогою спеціального ПЗ, що дозволяє дистанційного видаляти дані з пристрою у разі втрати або крадіжки;
- з метою фізичної безпеки, співробітники зобов'язані забезпечувати схоронність портативних пристроїв, не допускати втрати і приймати всі можливі заходи для запобігання крадіжки обладнання, не залишати пристрої без нагляду. Забороняється залишати пристрої без нагляду в місцях, куди можуть отримати доступ сторонні особи, залишати незаблокованими за допомогою замка в офісі, в готелі, в поїзді, в аеропортах і т. д. Необхідно використовувати спеціальні замки або інші засоби для захисту обладнання;
- забороняється залишати обладнання без нагляду в автомобілі.
- у разі втрати або крадіжки портативного обладнання (ноутбука, мобільного телефону, КПК і т. д.) працівник зобов'язаний в оперативному порядку повідомити свого Керівника та Департамент ІТ для своєчасного застосування заходів щодо запобігання витоку інформації. Такими заходами можуть бути - віддалене очищення носіїв пристрою, блокування доступу до пристрою і т. д.;
- у разі втрати обладнання порядок відшкодування моральної шкоди визначається уповноваженим співробітником.

Для використання робочих станцій і ноутбуків визначені наступні правила:

- забороняється використовувати комп'ютерну техніку або IT сервіси компанії в особистих цілях;
- забороняється самостійне переміщення, відключення кабелів робочих станцій, розбирання корпусів робочих станцій і ноутбуків без відома та участі IT-персоналу;
- підключення та використання особистого обладнання (ноутбуків, ПК, мобільних пристроїв) в корпоративній мережі компанії заборонено. В окремих випадках можливо підключення до мережі обладнання партнерів за умови дотримання стандартів інформаційної безпеки і наявності погоджень з боку уповноважених осіб;
- за зовнішнім виглядом пристроїв не повинно бути зрозуміло, що обладнання належить організації. Для досягнення цієї мети заборонено відображати логотип або ім'я:
  - в процесі завантаження ОС або BIOS,
  - на шпалерах робочого столу ОС,
  - на екранній заставці ОС,
  - у вікні входу в систему;
  - вхід повинен бути захищений, щонайменше, паролем;
  - користувач системи, перед тим як покинути робоче місце повинен переконатися, що його сесія або обладнання не може бути використане іншою особою без процесу автентифікації в момент відсутності користувача - забороняється залишати дисплеї з відкритим вікном терміналу, без нагляду. На час відсутності користувача на робочому місці комп'ютер повинен бути заблокований користувачем самостійно - в ОС Windows за допомогою комбінації клавіш «CTRL-ALT-DEL + Enter» або поєднання клавіш «Windows + L». Знання та використання процедури блокування терміналу обладнання є відповідальністю користувача;

- бездротові адаптери, такі Wi-Fi або Bluetooth повинні бути вимкнені за замовчуванням і можуть бути включені тільки тоді, коли є необхідність в їх використання для підключення до мережі. На портативних ПК включення і відключення проводиться за допомогою спеціального перемикача або кнопки з відповідним позначенням;
- користувач може використовувати тільки корпоративне програмне забезпечення, необхідне для виконання своїх обов'язків. Установка програмного забезпечення повинна здійснюватися уповноваженим працівником IT персоналу, згідно з правилами і процедурами. Установка або поширення отриманого незаконним шляхом програмного забезпечення на робочих станціях заборонено. Зберігання і поширення текстової, аудіо - та відеоінформації, отриманої незаконним шляхом на робочих станціях заборонено;
- користувачам заборонено змінювати або відключати брандмауер, антивірусне ПЗ та інші параметри безпеки ОС і устаткування;
- користувач несе відповідальність за використання надійних паролів при використання засобів шифрування або будь-яких інших засобів потребують автентифікацію;
- вся інформація, що належить компанії (документи, файли) повинна зберігатися тільки на серверах, а не на робочій станції користувача. За втрату документів, поточна версія яких не зберігається на сервері, несе відповідальність користувач;
- спільне використання локальних дисків, CD/DVD приводів робочих станцій заборонене.

Віддалений доступ до мережі надається у відповідності з наступними вимогами:

- для віддаленого доступу до локальної мережі організації дозволяється використовувати лише робочі станції або ноутбуки, що належать організації. Ці ПК повинні бути в домені і управлятися співробітниками IT

персоналу. Забороняється використання для віддаленого підключення робочих станцій, які не знаходяться під контролем компанії;

- для використання віддаленого доступу повинні бути отримані погодження керівника користувача, керівника IT та спеціаліста з інформаційної безпеки згідно з процедурою. Користувач повинен захищати налаштоване для віддаленої роботи обладнання від втрати або крадіжки. У разі втрати або крадіжки обладнання, користувач зобов'язаний негайно повідомити про цей факт IT персонал.

У зв'язку з невеликими розмірами портативних пристроїв (телефонів, КПК, USB-флешки тощо) та їх здатності зберігати великий обсяг інформації, ці пристрої повинні бути належним чином захищені:

- користувачам не дозволяється встановлювати на мобільні телефони або КПК, що належать компанії, несанкціоновані програми;
- доступ до мобільного телефону або КПК, що належить компанії або містить інформацію організації, повинен бути захищений паролем. Пароль доступу до КПК повинен бути встановлений як на включення так і на розблокування екрану;
- якщо це не є необхідним за роду діяльність співробітника, заборонено використовувати мобільні телефони або КПК для зберігання інформації, в тому числі повідомлень електронної пошти;
- забороняється зберігати інформацію, що належить компанії, на особистих пристроях, включаючи повідомлення електронної пошти;
- будь-яка інформація в мобільних телефонах, КПК і портативних пристроях зберігання інформації повинна зберігатися в зашифрованому вигляді, доступ до пристрою повинен здійснювати з використанням пароля;
- мобільні телефони і КПК, що належать організації, заборонено підключати до будь-яких інших пристроїв, які не знаходяться під контролем організації (персональні комп'ютери, комп'ютери в інтернет-кафе, друкарні тощо);

- щоб уникнути зберігання інформації на переносних носіях для обміну файлами між користувачами необхідно використовувати загальний мережний диск (сервер). Портативні USB-флешки» та інші записувальні пристрої призначені тільки для передачі інформації у випадках, коли іншої можливості не передбачено. «USB-флешки» та інші записувальні пристрої не можуть бути використані для довготривалого зберігання даних. За видалення інформації з «USB-флешки» при відсутності в необхідності її зберігання є сам користувач. Чутливі дані при передачі з використанням «USB-флешки» повинні бути захищені кодуванням;
- для передачі конфіденційної та секретної інформації за межі організації заборонено використовувати особисті записуючі пристрої, оскільки вони не знаходяться під контролем.

При роботі з даними, користувач повинен приймати ряд заходів для запобігання ризику втрати даних, таких як:

- для зберігання чутливих даних використовувати сервіс мережевих дисків, резервування даних на яких відбувається у відповідності з регламентом, а не зберігати файли на ноутбуці або робочій станції. Дані на локальних дисках ноутбуків і робочих станцій не резервуються, тому не можуть бути відновлені в випадку втрати;
- збитки при виході з ладу робочої станції або ноутбука включають збитки від втрати критичною інформації, що зберігається на ньому, які часто перевищують вартість заміни обладнання. При синхронізації (обмін інформацією між комп'ютером/КПК/сервером), з використанням технологій Bluetooth, Wi-Fi, IrDA або будь-який інший бездротової передачі даних, повинні використовуватися інструменти шифрування даних.

Робота з електронною поштою повинна здійснюватися з дотриманням таких правил:

- обліковий запис електронної пошти призначений тільки для службового використання;

- використання у службових цілях облікових записів електронної пошти, які не належать домену організації заборонено;
- використання автоматичної пересилання повідомлень електронної пошти на особисті адреси електронної пошти заборонено;
- при передачі повідомлень електронної пошти великій групі людей, серед яких наявні один або кілька зовнішніх одержувачів (осіб не з компанії), необхідно використовувати функцію "прихованої копії";
- забороняється відкривати та пересилати підозрілі вкладені файли (невідомий або підозрілий відправник, підозрілий вміст або вкладення електронної пошти) або відповідати на такого роду повідомлення. Також заборонено натискати посилання (відвідувати сайти), які представлені в підозрілих повідомленнях електронної пошти;
- забороняється створювати і пересилати ланцюжки повідомлень електронної пошти, в яких адресат просить переслати повідомлення як можна більшій кількості одержувачів, незалежно від причини, зазначеної в електронному листі підозрілого відправника (наприклад, для реєстрації в різних дискусійних групах, форумах або для доступу до сайтів, які вимагають реєстрації, і т. д.;
- будь-яка конфіденційна або таємна інформація при передачі електронною поштою за межі мережі організації повинна бути зашифрована перед передачею, наприклад з використанням архіватора з установкою пароля на архів;
- забороняється поширювати повідомлення електронної пошти, які є незаконними, несуть образливий або непристойний характер, містять наклеп або містять інформацію, яка може розглядатися як переслідування за ознакою статі, раси, національності, інвалідності, релігії або будь-яких інших форм меншин;

- перед відправкою конфіденційних або секретних даних одержувачу співробітник повинен упевнитися в особі одержувача, а також його праві отримання доступу до такої інформації.

Користувачеві в його відсутність рекомендується використовувати автоматичний відповідь, функцію «Поза офісу» або функцію делегування прав до своєї поштової скриньки відповідальному співробітнику.

Використання публічної мережі Інтернет здійснюється за такими правилами:

- доступ в Інтернет повинен здійснюватися тільки з використанням сервісів та IT інфраструктури компанії. При підключенні до Інтернет через стороннього провайдера, користувач повинен попередньо віддалено підключитися до мережі організації (з використанням VPN), а потім переглядати Інтернет з використанням інфраструктури і проксі-серверів компанії;
- Інтернет повинен використовуватися для службових цілей. Використання мережі інтернет в особистих цілях обмежена, так як використовувані при цьому ресурси обмежені (робочий час, пропускна здатність мережі). Використання мережі інтернет не має відбиватися на якості виконання працівником службових обов'язків або наносити збиток безпеки і бізнесу в будь-якій формі;
- завантаження медіафайлів або документів на офісні ПК в особистих цілях заборонено. Завантаження файлів (документів тощо) з інтернету може здійснюватися, лише якщо це необхідно для досягнення цілей Бізнесу та проводитися з урахуванням вимог законодавства. Зокрема, уникнення порушення авторських прав є відповідальністю працівника;
- забороняється завантаження і запуск з мережі Інтернет будь-яких виконуваних файлів (розширення *.exe);
- будь-яке незаконне, неправомірне або неналежне використання мережі Інтернет суворо заборонено;

- відвідування веб-сайтів, які можуть містити шкідливий код або нести ризик загрози зараження вірусами або поширення шкідливих програм забороняється. За рішенням менеджера з безпеки інформації деякі сайти можуть бути заблоковані;
- забороняється зберігати інформацію непристойного або образливого характеру на робочих станціях або файлових серверах компанії;
- у випадках появи «спливаючих вікон» або появи форми, що вимагає введення даних, потрібно бути пильними і упевнитися в достовірності ресурсу інтернет (адреси інтернет), необхідності введення таких даних, а в разі підозр не вводити свої особисті дані (можливі випадки шахрайства, соціальної інженерії);
- інтерактивні сервіси Інтернет, такі як інтернет-форуми, групи новин і каталогів можуть використовуватись тільки для службових цілей (отримання необхідної інформації);
- забороняється надавати і публікувати в мережі Інтернет і соціальних мережах (таких як Facebook, MySpace, Twitter, ВКонтакте і т. д.) вираження думки або інформації про організацію, а також клієнтів, продуктів, стратегій і т. д. Зазначені дії є відповідальністю уповноважених працівників спеціалістів з маркетингу і комунікацій, будь-які винятки з цього правила повинні бути затверджені уповноваженим співробітником;
- використання двох або декількох одночасних мережевих підключень з використанням різних пристроїв (модем, дротове або бездротове з'єднання) на персональних комп'ютерах і ноутбуках, заборонено. Перед підключенням до локальної мережі організації бездротові або модемне з'єднання повинні бути розірвані;
- передача будь-якої загальнодоступної інформації, а також файлів з використанням програм миттєвого обміну повідомленнями (ICQ, MSN і т. д.) з робочих станцій заборонено. Наявність будь-якого ПО для обміну файлами (P2P, торренти і т. д.) або їх використання на робочих станціях суворо

заборонено. Для цілей контролю даний клас може бути заборонений на запуск і завантаження на робочі станції співробітників.

З метою захисту від шкідливих програм співробітники компанії зобов'язані:

- не змінювати (тим самим послаблюючи захист) і не зупиняти антивірусне ПЗ або його модулі, зокрема, суворо забороняється деактивувати модуль отримання оновлень антивіруса;
- у разі підозри на вірус негайно інформувати про це IT персонал, а також фахівця з інформаційної безпеки. Виявлення вірусу на робочих станціях вважається інцидентом. Робочі станції, обладнання та системи повинні бути відключені від мережі, якщо є підозра, що вони піддаються нападу вірусів. Співробітники не повинні самостійно без участі IT виробляти чистку зараженого вірусом ПК, оскільки це може призвести до втрати інформації або подальшого поширення вірусу в мережі.

Співробітники компанії визнають, що уповноважені співробітники (внутрішній аудит менеджера з безпеки, тощо), з метою моніторингу, мають право здійснювати види діяльності відносно ПК або іншого обладнання, що належить компанії:

- збереження знімків екрану робочих станцій користувачів;
- перегляд списку встановлених програм;
- моніторинг використання мережі Інтернет;
- моніторинг і ведення архіву повідомлень корпоративної електронної пошти;
- безперервний моніторинг роботи обладнання та операційної системи робочої станції;
- будь-яку іншу діяльність, пов'язану із здійсненням контролю діяльності співробітників в мережі.

Користувач не може використовувати ПЗ або будь-які інші інструменти, які роблять неможливим або ускладнюють контроль робочих станцій.

Надання доступу працівникам до IT ресурсів і сервісів описуються відповідними процедурами. Будь-які зміни в правах доступу користувачів відбуваються згідно з відповідними процедурами і включають етапи узгодження з керівником підрозділу і власником ресурсу.

Ця політика визначає вимоги до складності пароля, правила поводження з паролем і процес автентифікації в системах. Для тих систем, які не генерують фіксовані паролі, користувач повинен самостійно вибрати пароль для свого облікового запису згідно з вимогами, наведеними нижче:

- мінімальна довжина пароля - 8 символів;
- складність - пароль повинен містити не менш ніж три символів із наступних груп:
  - прописні букви,
  - малі літери,
  - цифри,
  - спеціальні символи;
- пароль не повинен складатися з простих слів, не повинен містити інформацію ім'я користувача, імена членів сім'ї, дати народження тощо) і не повинен бути заснований на послідовностях, що легко підбираються (наприклад, ааааа, QWERTY, 123456 і т. д.);
- максимальна тривалість дії пароля - 60 днів (тобто обов'язкова зміна пароля протягом 60 днів);
- мінімальна тривалість строку дії пароля - 1 день;
- історія паролів - це неможливість використання останніх 13 паролів

Обліковий запис користувача блокується після 3 невдалих спроб входу в систему. Термін блокування облікового запису 15 хвилин.

Обліковий запис має обмежений круг ПК, на яких може бути виконаний вхід за його допомогою.

Співробітники зобов'язані належним чином поводитися зі своїми обліковими даними. Всі працівники та користувачі IT систем AXA повинні дотримуватися наступних правил:

- пароль або PIN-код є секретною інформацією та не підлягає розголошенню третім особам;
- співробітники не повинні записувати свій пароль або PIN-код в файлах або на папері (стікерів), а якщо пароль зафіксований в такій формі, то співробітник повинен забезпечити відповідні заходи безпеки для захисту і запобігання отримання доступу сторонньою особою (зберігати в закритому приміщенні або у зашифрованому вигляді);
- облікові записи користувачів створюються з тимчасовим паролем, дійсним на мінімальний термін, необхідний для зміни пароля на новий користувачем самостійно. Користувач повинен змінити пароль після першого входу в систему;
- у разі розголошення паролів або підозри, що розкриття сталося, співробітник повинен відразу ж змінити пароль і згідно з даною політикою - «Управління інцидентами інформаційної безпеки», повідомити про цей інцидент IT персонал.
- один і той же пароль не може бути використаний у різних IT системах. Категорично забороняється використовувати пароль для IT систем Компанії в інших системах за межами компанії (особливо в Інтернеті, наприклад, для особистої електронної пошти);
- знати і виконувати ці правила використання є обов'язком співробітника. Користувач несе повну відповідальність за дії, виконані від імені його облікового запису в системах, в такому випадку дії інтерпретуються як дії співробітника.

Перегляд прав доступу до всіх інформаційних систем повинен здійснюватися власником системи (представник Бізнесу, володіє системою) по можливості два рази, але не рідше ніж один раз на рік. Перегляд

адміністративних прав доступу користувачів до своїх ПК, у разі наявності такого списку винятків, повинен також переглядатися не рідше ніж один раз на рік. Більш глибоко процедура описана у відповідному розділі.

Процес управління змінами в ІТ системах є частиною «Життєвого циклу розробки та впровадження в експлуатацію ІТ систем».

Концепція користувальницьких обчислювальних систем (КОС) включає в себе рішення приватних завдань користувачів ПК - з допомогою локальних баз даних, електронних таблиць, сценаріїв і т. д. КОС являє діяльність, пов'язану із створенням, вдосконаленням, придбанням і експлуатацією користувацьких додатків, ці програми не управляються централізовано ІТ персоналом. Власник (оператор, користувач) КОС в частині практичного застосування цього ПЗ несе відповідальність за:

- підходи до управління або використання,
- резервне копіювання,
- управління змінами (локальні налаштування),
- відповідність технічним стандартам.

Відповідальністю користувачів КОС є правомірне використання даного класу ПЗ у відповідності до цієї політики і використання тільки затвердженого Департаментом ІТ програмного забезпечення. Користувач прикладного ПЗ несе відповідальність за підтримку даного класу.

Інцидент інформаційної безпеки - це подія, в результаті, якої мають місце або можуть бути порушення інформаційної безпеки, тобто подія, що призвела або могла призвести до порушень конфіденційності, цілісності або доступності інформації в електронній чи будь-якій іншій формі. З метою забезпечення безпеки інцидент вважається спробою подолання заходів безпеки або політики безпеки.

Найбільш поширені інциденти інформаційної безпеки:

- невідповідне використання - порушення інформаційної безпеки або інших правил безпеки (розкриття паролів, недостатній захист документів,

завантаження, установка або запуск будь-якого несанкціонованого ПЗ, відкриття підозрілих вкладень електронної пошти і т. д.);

- вірусне зараження - інцидент інформаційної безпеки в результаті появи черв'яків, троянських коней та інших шкідливих програм, які заразили комп'ютер - інцидент, як правило, відбувається в результаті порушення правил безпечної роботи;
- несанкціонований доступ - ситуація, в якій неуповноважена на те особа отримує (або намагається отримати) логічний чи фізичний доступ до мережі, системи, додатку, даних або інших джерел інформації організації;
- втрата - втрата даних, інформації, медіа-даних, програмного забезпечення чи технічних засобів;
- відмова в обслуговуванні - інцидент інформаційної безпеки, який блокує або обмежує дозволене використання мереж, систем або додатків внаслідок виходу з ладу окремих вузлів інфраструктури ІТ. Це може бути відмова ІТ обладнання, помилки адміністратора або атака на інфраструктуру і т. д.;
- соціальна інженерія - несанкціоновані спроби зловмисників електронною поштою або по телефону, схилити співробітників організації до розголошення конфіденційної інформації або здійснити дії, які можуть призвести до розкриття конфіденційної інформації, або впровадження шкідливого програмного забезпечення - як правило, з проханням запустити файл, що відправлений електронною поштою або запуск користувачем додатків, або відкриття файлів на знайденій "флешці" (USB-накопичувач) і т. д.

У разі виникнення інциденту, в тому числі підозри в тому, що трапився інцидент, співробітник повинен повідомити про це ІТ персонал та спеціаліста по інформаційної безпеки. Якщо в результаті інциденту, співробітник отримав доступ до інформації, до якої не має мати доступ, працівник повинен повідомити про це ІТ персонал і спеціаліста з інформаційної безпеки.

Користувач повинен надавати всю можливу допомогу в оцінці збитку і пом'якшення наслідків, які повинні, зокрема:

- бути в змозі ідентифікувати будь-яку необхідну інформацію і, якщо можливо забезпечити її відновлення з інших джерел;
- бути в змозі ідентифікувати інформацію, розголошення якої несе великі ризики, і вжити заходів щодо мінімізації наслідків її розкриття;
- бути в змозі забезпечити захист даних та інформації, необхідної для аналізу інциденту.

В даний час інформація є настільки важливим ресурсом, що її захист виходить на перший план практично в кожній компанії, інформація є критично важливою. В наслідок цього, крім одноразового впровадження систем захисту інформації, так само необхідні періодичні заходи для підтримки і поліпшення цієї системи.

Перегляд прав доступу проводиться для уникнення витоку інформації шляхом отримання кимось несанкціонованого доступу до інформації компанії. В умовах достатньої плинності кадрів і тенденції бізнесу, що змінюється. Дана процедура є необхідною для забезпечення інформаційної безпеки.

Масштаб - це сукупність систем і ресурсів, на які розповсюджується процедура перегляду прав доступу користувачів і співробітників. У цю область входять:

- платформи 1С та доступ до звітів в них;
- доступ до сервісів, тип доступу до інтернету, доступ до зовнішніх ресурсів, доступ до корпоративних даних ззовні компанії через web і мобільних додатків;
- фізичний доступ в офісні приміщення;
- віддалений доступ (remote access VPN, AD).

Власником даних є особа, головним чином зацікавлена у збереженні даної інформації, а точніше до збереження її конфіденційності, доступності та цілісності.

Власником системи є співробітник, метою якого є збереження працездатного стану ІТ системи. У деяких випадках роль власника даних або системи може виконувати уповноважений працівник, приміром директор департаменту.

Власник системи/даних несе відповідальність за захист даних у системі, тому будь-які зміни в правах доступу узгоджуються з ним.

Менеджер з інформаційної безпеки ініціює процедуру перегляду прав доступу в ІТ системі, відправляючи запит власнику системи/даних на відповідність прав доступу співробітникам. Після підтвердження або спростування приналежності прав доступу співробітник ІТ департамент надає або обмежує права доступа зазначеним співробітникам.

Дана процедура повинна проводитися не рідше ніж один раз на рік. При появі інцидентів в системі, або прояві будь-яких інших непередбачених випадків перегляд прав доступу може проводитися позапланово.

ІТ система складається з безлічі різних компонентів, кожен з яких має свої захищені та вразливі місця. І будь-яке з цих вразливих місць може стати вразливістю для ІТ системи. Тому для забезпечення працездатності системи необхідно здійснювати контроль і управління даними недоліками, а в наслідок і уразливими.

Управління вразливостями поширюється на наступні компоненти:

- WEB-ресурси та інші критичні компоненти;
- клієнтські і серверні ОС;
- мережеві пристрої;
- інші вузли інфраструктури ІТ.

Методологія проведення оцінки вразливостей ІТ системи складається менеджером інформаційної безпеки і може ґрунтуватися на таких відкритих джерелах як OSSTMM 3, SP800-115(NIST).

Для тестування рекомендується, використовувати одні із найпоширеніших аналітичних програмних продуктів у сфері інформаційної безпеки:

- Nessus;
- Windows Security Compliance manager;
- Microsoft Baseline Security Analizer.

Процес управління вразливостями є складним, тому складається з декількох етапів (рис. 3.1):

Рис. 3.1. Процес управління вразливостями IT

- Підготовка

Scanning scope - Визначення сфери охоплення

На даному етапі менеджер з інформаційної безпеки визначає компоненти системи, що підлягають скануванню на уразливості.

Owner approve - Підтвердження власником

Набір компонентів, що підлягають скануванню, передається власникові системи/даних на розгляд. Власник зобов'язаний або підтвердити перелік сканованих компонентів, або створити рекомендації щодо його коригування.

- Сканування на вразливості

Action – Сканування

Кожен компонент IT системи, визначений в області охоплення сканується на уразливості відповідними інструментами.

Report – Звіт

За результатами сканування формується звіт про знайдені вразливості. Звіт повинен містити детальний опис кожної знайденої вразливості і рекомендації до їх усунення.

- Визначення пом'якшуючих дій

Грунтуючись на звіті про знайдені вразливості і рекомендації по їх усуненню створюється план зміни IT системи, призначений для усунення всіх знайдених вразливостей.

- Застосування пом'якшуючих дій

IT департамент виконує всі зміни системи, визначені в плані дій і надає звіт по зробленим діям.

- Повторне сканування

Після впровадження всіх змін проводиться повторне сканування компонентів, визначених в області охоплення для підтвердження усунення знайдених раніше вразливостей.

- Період повторення

Дана процедура повинна проводитися не рідше одного разу в квартал. При виникненні непередбачуваних ситуацій, інцидентів або появі нового типу загроз може проводитися позапланова перевірка IT мережі на вразливості.

Процедура перегляду правил мережевих екранів і конфігурації мережі проводиться для підтримання безпеки налаштувань мережевих компонент.

Scope - Область охоплення. Компоненти, які вимагають перегляду правил і конфігурації наступні:

- мережеві пристрої другого і третього рівнів (комутатори, маршрутизатори), мережеві екрани (Cisco ASA);

- Firewall & Proxy (перегляд/створення/зміна існуючих/видалення неактуальних access-листів);
- Network Blueprint Update (підтримання актуальності карти мережі);

Процес. Менеджер з інформаційної безпеки ініціює цю процедуру у відповідності з графіком проведення відповідних заходів, і виконує її разом з відповідальним персоналом департаменту IT.

Період повторення. Дана процедура повинна виконуватися не рідше одного разу на рік. При виникненні непередбачених ситуацій або інцидентів може проводиться позаплановий перегляд правил мережевих екранів і конфігурації мережі (табл. 3.1).

Таблиця 3.1

Опис	Регулярність	Відповідальний
Перегляд прав доступа в IT мережі	не менше 1 раза на рік	Менеджер з безпеки
Управління вразливостями	не менше 1 раза на квартал	Менеджер з безпеки
Перегляд прав мережевих екранів і конфігурації мережі	не менше 1 раза на рік	Менеджер з безпеки

Незважаючи на всі вбудовані системи захисту інформації та планові періодичні заходи по її підтримці, збереження даних все одно перебуває під загрозою, будь то від якихось нових способів проникнення зловмисників у систему, про яких ще не «знає» наша система, або від звичайних збоїв в IT системі. Беручи до уваги принцип безперервності бізнесу, для повноцінного збереження даних, крім описаних вище засобів захисту інформації так само постійно діючі заходи, такі як управління актуальними інформаційними ризиками. Даний процес припускає визначення ризиків для IT системи, їх оцінку і прийняття заходів по захисту від цих ризиків або прийняття їх на себе.

План заходів контролю наведений у табл. 3.2.

Таблиця 3.2

Опис	Регулярність	Відповідальний
Контроль використання замків безпеки для ноутбуків і блокування екранів робочих станцій	Не менше одного разу на протязі року	LSO
Перевірка встановленого програмного забезпечення на робочих станціях користувачів	Не менше одного разу на протязі року	LSO, CIO
Контроль за дотриманням правил "політики чистого робочого столу"	Не менше одного разу на протязі року	Керівники, LSO
Інші адміністративні і технічні заходи контролю	Не менше одного разу на протязі року	LSO
Інструменти контроля, визначені згідно з річним планом аудита	Згідно плану	Функція IT аудиту

Власником ризику є власник активу, схильного до ризику. Власник відповідає за його обробку.

Процес управління інформаційними ризиками є складним і включає в себе:

- Оцінка ризиків. Метою оцінки ризиків є кількісна оцінка рівня ризику. Ризик повинен бути виражений як комбінація результату від впливу ризику та ймовірності його реалізації.
- Оцінка частоти (ймовірності). Значення ймовірності реалізації ризику може ґрунтуватися на статистичній інформації про конкретний об'єкт (якщо ця інформація доступна) або може бути визначена в результаті експертної оцінки.

Табл. 3.3 надає діапазон значень, які будуть використовуватися для оцінки ймовірності.

Таблиця 3.3

Приклад		Частота/вірогідність
-	Завжди	Завжди
Відбувається часто	Декілька разів на рік	Дуже вірогідно
Повторюється знову. Подія відома, може повторитись на протязі декількох років	Один раз на рік або раз в п'ять років	Вірогідно
Дуже нечасто і навряд відбудеться	Не більше раз в 10 років	Не часто
-	Ніколи	Ніколи

Оцінка впливу. Оцінка впливу ризику визначає потенційні наслідки події. Цей розрахунок ґрунтується на таблиці оцінки збитку (Severity Assessment Table - SAT). Отримані дані зводяться до таблиці (табл. 3.4):

Таблиця 3.4

Результат із SAT	Результат оцінки взаємодії
A	Найбільш серйозна шкода
B	Дуже серйозна шкода
C	Серйозна шкода
D	Невелика шкода
E	Незначна шкода

Визначення результатів аналізу ризику. Після визначення ймовірності події та впливу на бізнес, в менеджера з інформаційної безпеки є можливість розрахувати рівень ризику. Наступна матриця представляє границі для класифікації рівнів ризику (рис. 3.2).

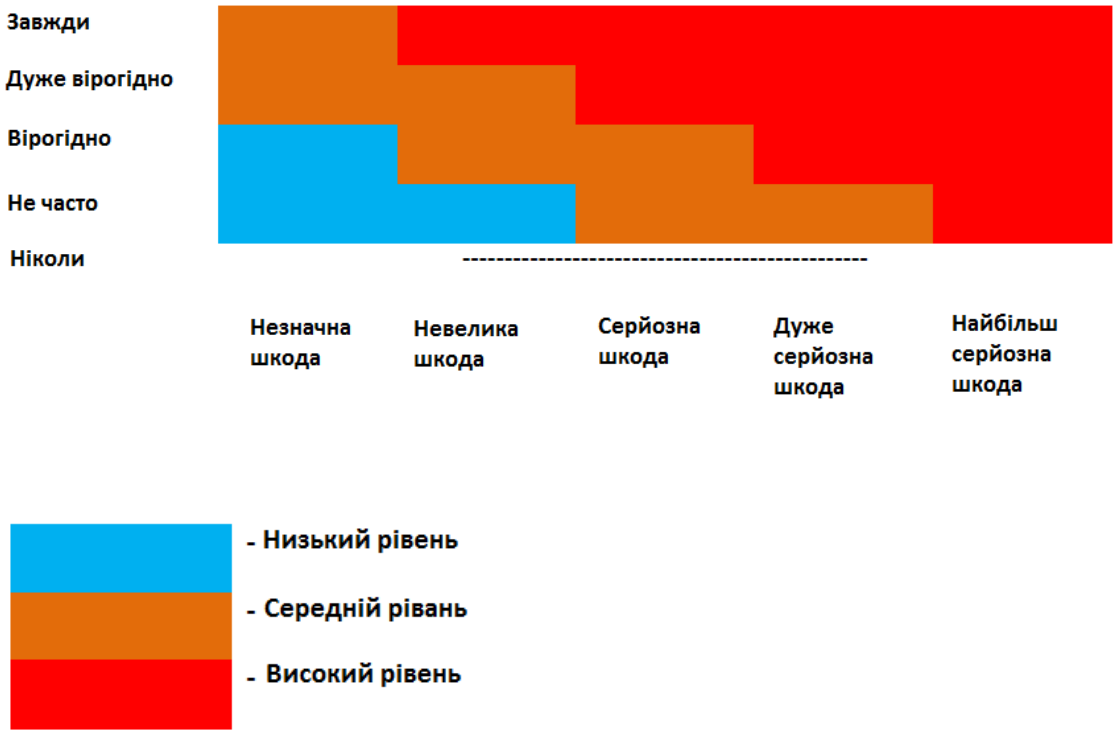

Рис. 3.2. Класифікація рівнів ризику інформаційної безпеки

Загальна оцінка ризику повинна виконуватись із залученням фахівців з відповідним рівнем технічного і бізнес досвіду. Для винесення остаточного рішення при оцінці втрати, менеджер з інформаційної безпеки повинен залучити відповідного власника ризику.

Для оцінки ризиків з високим рівнем або коли неможлива оцінка частоти і ймовірності події, ці показники приймаються як «Ймовірно». В такому випадку оцінка ризику проводиться за наступною матрицею (рис. 3.3):

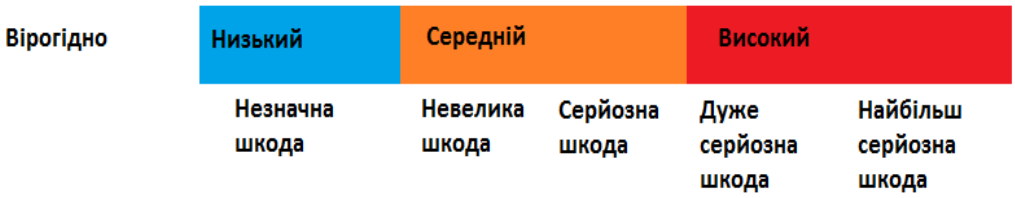

Рис. 3.3. Матриця оцінки ризику інформаційної безпеки

- Обробка ризиків. Якщо оцінка рівня ризику вище ніж «Низький», дії щодо його усунення є обов'язковими. Ці дії повинні:

а) якщо можливо, усунути першопричини ризику;

б) зменшити ймовірність і/або вплив ризику на бізнес.

Менеджер з інформаційної безпеки повинен співпрацювати з власником ризику для визначення плану дій щодо усунення ризику. План дій повинен:

а) визначати необхідні бюджет і ресурси;

б) призначити дати виконання плану;

в) визначити ролі та обов'язки за зазначені дії.

- Прийняття ризиків. Якщо план пом'якшення впливу ризику не встановлено, або якщо бюджет і ресурси недоступні, власник ризику і керівник компанії повинні формально прийняти існуючий ризик, підписавши форму прийняття ризику (Risk Acceptance Form - RAF). З прийняттям ризику, керівництво стверджує своє розуміння про потенційний вплив ризику. Форма прийняття ризику (RAF), після підписання, повинна бути відсканована і збережена у цифровому вигляді для зберігання.

- Моніторинг та розгляд ризиків. Менеджер з інформаційної безпеки повинен один раз у квартал проводити моніторинг існуючих інформаційних ризиків, незалежно від стадії прийняття та намічених пом'якшуючих планів дій. Уся необхідна інформація збирається в рамках процесу управління інформаційними ризиками і поміщається в реєстр інформаційних ризиків. Реєстр необхідно періодично переглядати, що б переконатися в проведенні намічених дій. Форми прийняття ризиків повинні регулярно переглядатися щодо можливості зміни відповідних контролів. Дана діяльність повинна виконуватися мінімум один раз в квартал або частіше, якщо буде потрібно. Менеджер з інформаційної безпеки відповідає за збір необхідної інформації для огляду реєстру ризиків. Під час фази моніторингу менеджер з інформаційної безпеки проводить переоцінку ризиків і форм прийняття ризику. Переоцінка

може забезпечити більш точне розуміння ситуації. У разі прийняття ризику, підписана форма прийняття ризику визначає дату обов'язкової переоцінки.

Власник додатків відповідає за:

- правильне функціонування програми в цілому;
- визначення та забезпечення реалізації відповідних заходів щодо забезпечення безпеки;
- затвердження запитів на зміни, які стосуються нової функціональності та їх пріоритезацію.

Власник даних (інформації) (data owner) - зазвичай керівник відповідного підрозділу, який несе персональну відповідальність за захист та використання певної інформації.

Власник даних проявляє необхідну турботу про інформацію та несе відповідальність за будь-які халатні дії, спотворення або розголошення інформації.

Власник даних приймає рішення щодо класифікації інформації та зобов'язаний своєчасно переглядати рівень класифікації у разі зміни потреб бізнесу. Також він повинен забезпечити впровадження необхідних заходів безпеки, переконатися в правильному розмежуванні прав доступу, сформулювати вимоги безпеки згідно з класифікацією, а також вимоги щодо організації резервного копіювання інформації, погоджувати будь-які дії за санкціонованою розголошенню (передачі) інформації, визначати критерії доступу до інформації.

Власник даних погоджує запити на доступ до інформації, але може делегувати цю функцію одному з нижчестоящих керівників свого підрозділу. Власник даних делегує обов'язки по щоденній підтримці механізмів захисту даних відповідального за зберігання даних. В власниками даних є:

- в «чистому» вигляді - Керівник Організації (CEO);
- дані після специфічної обробки (вибірки) - відповідні члени Правління (C-level - CFO, COO та інші)

Власник даних може делегувати свої обов'язки іншій особі, проте відповідальність за прийняті рішення залишається за Власником даних.

Кожен керівний працівник повинен контролювати і забезпечувати дотримання всіх положень політики інформаційної безпеки в своєму секторі, зокрема:

- бути впевненим, що відправлення або одержання чутливих даних про клієнтів, партнерів та ін.) поза мережі організації електронною поштою або за допомогою інших електронних засобів, проводиться в захищеному вигляді (наприклад, з використанням пароля на архіви);
- забезпечити, при взаємодії з будь-якою третьою стороною (партнерами, постачальниками, сервісними організаціями, аудиторами тощо) підписання договору про нерозголошення інформації у разі роботи з конфіденційними даними організації. Третя сторона повинна розглядати таку інформацію в відповідно до стандартів і політики інформаційної безпеки компанії.
- проводити періодичну (не менш одного разу в рік) перевірку прав доступу своїх підлеглих у системах, їх актуальність, відповідність посади та службової необхідності.

Керівники повинні виступати прикладом для своїх підлеглих при операціях з чуттєвими даними і слідувати вказаним в політиці правилам (використовувати замки безпеки для ноутубків, блокувати екран, дотримуватися «політику чистого робочого столу» і т. д.).

Кожен співробітник зобов'язаний:

- ознайомитися з усіма правилами і процедурами, які застосовуються для захисту інформації, та дотримуватися їх;
- розвивати свої навички в області захисту інформації, що відповідають його ролі і позиції в компанії.

За невиконання вимог Політики інформаційної безпеки співробітники компанії і партнери несуть перед компанією дисциплінарну,

матеріальну та кримінальну відповідальність згідно з законодавством.

3.2. Пропозиції щодо функціонування документу «Політика інформаційної безпеки» на підприємстві

На сучасному етапі розвитку ІБ на підприємствах України існують наступні проблеми, що стосуються документу «Політика інформаційної безпеки»:

- недостатня обізнаність співробітників в комп'ютерних технологіях та зокрема в інформаційній безпеці;
- нехтування положеннями, наведеними в документі;
- відсутність розуміння у керівників середнього та нижнього рангу, а також у персоналу необхідності проведення робіт по підвищенню рівня інформаційної безпеки.

Оскільки не кожен із співробітників має належні знання у сфері комп'ютерних технологій та інформаційної безпеки, існує ризик порушення певних пунктів, вказаних в документі «Політика інформаційної безпеки». Наприклад, зараз є дуже поширеним є черв'як, що надходить як спам-лист з вкладенням формату .cab. При запуску цього вкладення він незворотно зашифровує всі офісні документи на комп'ютері (в томі числі інформацію на мережевих дисках, до якої обліковий запис користувача має доступ). Нажаль жоден із сучасних антивірусів не виявляє шкідливого коду в такого виду файлах. Допомагає лише відновлення файлу з раніше зробленої резервної копії. Нажаль через незнання співробітники можуть запустити цей файл.

Таким чином, для забезпечення достатнього рівня дотримання правил політики інформаційної безпеки необхідно проводити тренінги та семінари, що дозволять підвищити обізнаність співробітників компанії у даній сфері. Тренінги можна робити в режимі он-лайн за допомогою перегляду деякого відео-матеріалу. Закінчувати було б не погано невеликим тестом для перевірки засвоєнням інформації. Також необхідно періодично надсилати електронною

поштою співробітникам матеріали щодо інформаційної безпеки для ознайомлення, розклеювати наочний матеріал на дошках оголошень.

Деякі співробітники можуть нехтувати положеннями, що зазначені в документі «Політика інформаційної безпеки». Причиною може бути багато, наприклад, не задоволеність стандартами корпоративного програмного забезпечення (користувач може завантажити на ПК портативну версію програми і користуватися нею), потреба у використанні інтернету у власних цілях, тощо.

Для контролю та забезпечення дотримання правил, вказаних у політиці, можна використати деяке програмне забезпечення і настроювання робочої станції користувача.

Наведемо приклади ПЗ і можливості.

- для забезпечення надійного і контрольованого доступу до інтернету користувачів можна використовувати проксі сервер. Наприклад Forefront Threat Management Gateway. За допомогою програмного комплексу ми можемо обмежувати доступ до сайтів, обмежувати швидкість роботи з інтернетом у користувачів, забороняти завантажувати файли по типу, при чому для кожної групи користувачів можливо створити свої правила. Також є можливість аудиту;
- для забезпечення контролю над додатками та доступу до переносних носіїв використовується Symantec Endpoint Protection (SEP). Данна програма являє собою як і антивірус, так і програмний комплекс для вирішення деяких проблем безпеки. Таким чином за допомогою даного програмного комплексу ми можемо заборонити запуск деяких програм, а також читання/запис на USB/CD/DVD;
- для розширеного розгортання програмних комплексів (того ж SEP) на велику кількість ПК не погано використовувати Microsoft System Center Configeration Manager. Дане ПЗ дозволяє як масово розгортати програмні

комплекси без відома користувача, так і служить хорошим інструментом для аудиту робочих станцій.

- для інших обмежень можна використовувати доменні політики (GPO). Наприклад, видалити ПЗ з комп'ютера, відключити на доменному ПК обліковий запис локального адміністратора, задати певні настройки для безпечності браузера, задати складність пароля користувачеві і т.д.
- для обмеження доступу до ресурсів на файловому сервері організації використовується Active Directory. Ми можемо надати чи надати права на певну інформацію користувачу або групі користувачів.

Деякі положення неможливо вирішити за допомогою ПЗ. Тому, на мою думку, необхідно включити підтвердження про ознайомлення з політикою безпеки організації і прийняття обов'язку її дотримуватися у трудовий договір, який співробітник підписує при працевлаштуванні.

Справа в тому, що на цій сходинці управлінської драбини, як правило, не видно стратегічних завдань, що стоять перед організацією. Питання безпеки при цьому можуть викликати також і роздратування – вони створюють «непотрібні» труднощі.

Як правило, наводяться наступні аргументи проти проведення робіт і прийняття заходів щодо забезпечення інформаційної безпеки:

- поява додаткових обмежень для кінцевих користувачів та фахівців підрозділів, що утрудняє користування автоматизованою системою організації;
- необхідність додаткових матеріальних витрат на проведення таких робіт, так і на розширення штату фахівців, що займаються проблемою інформаційної безпеки.

Зазначена проблема є однією з основних. Всі інші питання так чи інакше виступають в якості її наслідків. Для її подолання важливо вирішити такі завдання:

- підвищити кваліфікацію персоналу в області захисту інформації шляхом проведення спеціальних нарад, семінарів;

- підвищити рівень інформованості персоналу, зокрема про стратегічні завдання, що стоять перед організацією.

І насамкінець, варто зазначити, що для забезпечення інформаційної безпеки підприємства розробки документу «Політика інформаційної безпеки» недостатньо. Адже не кожен співробітник, навіть підписавши усі необхідні документи буде сумлінно дотримуватись кожного пункту загаданого вище документу.

Висновки до розділу 3

Документ «Політика інформаційної безпеки» підприємства повинен включати такі елементи як: загальні положення; мету та завдання політики інформаційної безпеки; основні напрями забезпечення інформаційної безпеки підприємства; система управління інформаційною безпекою на підприємстві; прикінцеві положення.

Сьогодні серед проблем, що стосуються функціонування документу «Політика інформаційної безпеки» підприємства є недостатня обізнаність співробітників в комп'ютерних технологіях та зокрема в інформаційній безпеці; нехтування положеннями, наведеними в документі та відсутність розуміння у керівників середнього та нижнього рангу, а також у персоналу щодо необхідності проведення робіт по підвищенню рівня інформаційної безпеки. Оскільки, не кожен із співробітників має належні знання у сфері комп'ютерних технологій та інформаційної безпеки, існує ризик порушення певних пунктів, вказаних в документі «Політика інформаційної безпеки». Для забезпечення достатнього рівня дотримання вимог документу «Політика інформаційної безпеки» необхідно проводити тренінги та семінари, що дозволять підвищити обізнаність співробітників підприємства у даній сфері.

ВИСНОВКИ

Під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури.

Політика інформаційної безпеки підприємства включає набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Політика інформаційної безпеки може бути викладена як на описовому рівні, так і за допомогою певної формальної мови. системи. Формальний вираз політики інформаційної безпеки називають моделлю політики інформаційної безпеки. Основна мета створення політики інформаційної безпеки й опису її у вигляді формальної моделі ─ це визначення умов, яким має підпорядковуватися поведінка підприємства, вироблення критерію безпеки і проведення формального доведення відповідності підприємства цьому критерію при додержанні встановлених правил і обмежень.

Метою розробки політики інформаційної безпеки на підприємстві є забезпечення підтримки інформаційної безпеки його керівництвом, яке повинно поставити чітку мету і всесторонньо подавати свою підтримку інформаційної безпеки за допомогою розповсюдження політики безпеки серед співробітників підприємства.

Процес захисту інформації являє собою взаємодію загроз інформації та інформаційної безпеки, що перешкоджає їхній взаємодії. Захист інформації відбувається поетапно і у свідомо певному порядку. Всі етапи об'єднуються в цілісну модель розподілу ресурсів для захисту інформації. Вона заснована на можливостях зловмисника і сторони, що захищається, на базі моделі загроз і моделі оцінки втрат. Це відбувається тому, що вартість захисту не повинна перевищувати шкоду порушення безпеки.

Основними моделями політики інформаційної безпеки є дискреційна, мандатна та рольова.

Документ «Політика інформаційної безпеки» підприємства повинен включати такі елементи як: загальні положення; мету та завдання політики інформаційної безпеки; основні напрями забезпечення інформаційної безпеки підприємства; система управління інформаційною безпекою на підприємстві; прикінцеві положення.

Сьогодні серед проблем, що стосуються функціонування документу «Політика інформаційної безпеки» підприємства є недостатня обізнаність співробітників в комп'ютерних технологіях та зокрема в інформаційній безпеці; нехтування положеннями, наведеними в документі та відсутність розуміння у керівників середнього та нижнього рангу, а також у персоналу щодо необхідності проведення робіт по підвищенню рівня інформаційної безпеки. Оскільки, не кожен із співробітників має належні знання у сфері комп'ютерних технологій та інформаційної безпеки, існує ризик порушення певних пунктів, вказаних в документі «Політика інформаційної безпеки». Для забезпечення достатнього рівня дотримання вимог документу «Політика інформаційної безпеки» необхідно проводити тренінги та семінари, що дозволять підвищити обізнаність співробітників підприємства у даній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Близнюк І. Науковий вісник Національної академії внутрішніх справ України. - 2013. - № 5. - С. 206-214 - (Інформаційна безпека України та заходи її забезпечення).
2. Богуш В. Інформаційна безпека держави / Володимир Богуш, Олександр Юдін,; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2015. - 432 с.
3. Бондарь И. Проблемы информационной безопасности в условиях переходного общества / И. Бондарь. - 2003. - № 8. - С. 47-48. - (Персонал)
4. Борсуковський Ю. Подходы и решения: Информационная безопасность. - 2011. - № 5. - С. 41-42 - (Мир денег).
5. Братель О. Поняття та зміст доктрини інформаційної безпеки . - 2006. - № 5. - С.36-40 - (Право України).
6. Бут В.В. Науковий вісник Національної академії внутрішніх справ України. - 2013. - № 5. - С. 225-232. - (Проблеми безпеки в інформаційній сфері - сутність понять та їх термінологічне тлумачення).
7. Гмурман, А.И. Информационная безопасность – М.: «БИТ-М». 2004. – 387 с.
8. Голубенко О.Л. Політика інформаційної безпеки. -Луганськ: вид-во СНК ім. В.Даля. 2009. – 300 с.
9. Горбатюк О.М. Вісник Київського університету імені Т.Шевченка. - 2009. - Вип. 14: Міжнародні відносини. - С. 46-48. - (Сучасний стан та проблеми інформаційної безпеки України на рубежі століть).
10. Грездов Г.Г. Модифицированный способ решения задачи нормирования эффективной комплексной системы защиты информации автоматизированной системы / Г.Г. Грездов; монография. – К.: ДУІКТ, 2009. – 32 с.
11. Гуцалюк М. Інформаційна безпека у сучасному суспільстві. - 2005. - № 7. - С.71-73. - (Право України).

12. Гуцалюк М. Інформаційна безпека України: нові загрози. - 2013. - № 5. - С. 2-3. - (Бизнес и безопасность).
13. Державна служба спеціального зв'язку та захисту інформації України. [Електронный ресурс] – Режим доступу до журн.: http://www.dstszi.gov.ua/dstszi/control/uk/index.
14. Домарєв В.В., – Безопасность информационных технологий. Персональный сайт к.т.н. Домарева В.В. [Електронный ресурс] – Режим доступу до журн.: http://www.security.ukrnet.net/modules/news/.
15. Закони України. -К., 1997.- Т.7. - (Про захист інформації в автоматизованих системах: Закон України від 5.07.1994 р.)
16. Захаров Е. Информационная безопасность или опасность отставания? - 2010. - № 1 . - С. 3-5. - (Права людини).
17. Ігнатьев В.А. Информационная безопасность современного коммерческого предприятия. – Старый Оскол: ООО «ТНТ», 2005. – 448с.
18. Інформатизація та відкритість влади як засоби демократизації суспільства. Зб. матеріалів «круглого столу» у Національному інституті стратегічних досліджень 17.12.2012 р. - 1С, 2003.
19. Інформаційна безпека України: проблеми та шляхи їх вирішення . - 2010. - № 1. - С. 60-69. - (Національна безпека і оборона).
20. Інформаційна безпека. [Електронний ресурс] - Режим доступу до журн.: http://uk.wikipedia.org/wiki/.
21. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами. - 2009. - № 2. - С. 15-17. - (Альманах економічної безпеки)
22. Конєєв И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб. БХВ-Петербург, 2003. – 752 с.
23. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич,. -К.: Кондор, 2005. -382 с.
24. Литвиненко О. Інформація і безпека. - 2008. - № 1. - С. 47-49. - (Нова політика).

25. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Ірина Маракова, Анатолій Рибак, Юрій Ямпольский,; Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій . -Одеса, 2011. -164 с.
26. Мельников В.П., – Информационная безопасность и защита информации./В.П. мельников, С.А. Клейменов, А.М. Петраков. – 3–е изд., стер. – М.: Издательский центр «Академия», 2008. – 336 с.
27. Національна безпека і оборона. - 2011. - № 1. - С. 16-28. - (Система забезпечення інформаційної безпеки України).
28. Остроухов В. До проблеми забезпечення інформаційної безпеки України. - 2008. - № 4. - С. 135-141. - (Політичний менеджмент).
29. Офіційний сайт Symantec. Отчет об угрозах безопасности в интернете. Том 17. [Електронный ресурс] – Режим доступу до журн.: http://www.symantec.com/ru/ru/threatreport/.
30. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. / Петренко С.А., Симонов С.В. – М.: Компания АйТи ; ДМК Пресс, 2014. – 384 с.: ил.
31. Пилипенко О. СНІР. - 2005. - № 12. - С. 72-73. - (Формула безопасности: Информационная безопасность).
32. Політика забезпечення інформаційної безпеки [Електронний ресурс] - Режим доступу до журн.: http://securitypolicy.ru/index.php/.
33. Правове забезпечення інформаційної діяльності в Україні/ Володимир Горобцов, Андрій Колодюк, Борис Кормич та ін.; Ред. І. С. Чиж; Ін-т держави і права ім. В.М.Корецького, Нац. Академія Наук України, Держ. комітет телебачення і радіомовлення України. -К.: Юридична думка , 2006. -384 с.
34. Про інформацію: Закони України. -К., 1996. Т.4. - (Закон України від 02.10.1992 р.).
35. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная

безопасность предприятия: Учебное пособие.2-е изд. ─М.: Издательско-торговая корпорация «Дашков и К°». 2005. ─ 336 с.

36. Устинов, Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий. – М.: Радио и связь. 2013. – 342 с.
37. Центр інформаційної безпеки [Електронный ресурс] – Режим доступу до журн.: http://www.bezpeka.com/files/lib_ru/book-domarev03/ch_08.pdf.
38. Цимбалюк В. Підприємництво, господарство і право. - 2004. - № 3. - С. 88-91. - (Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації)).
39. Цимбалюк В. С. Новий Кримінальний кодекс України: питання застосування і вивчення. Матеріали міжнар. наук.-практ. конф. 25-26 жовтня 2011 р. - Х.; К., 2012. - С 167-170. - (Категорія «безпека» у новому Кримінальному кодексі України).
40. Чубарук Т. Право України. - 2007 . - № 9 . - С. 67 – 69. - (Проблеми законодавчого забезпечення інформаційної безпеки в Україні).
41. Щербина В. М. Актуальні проблеми економіки. - 2006. - № 10. - С. 220 - 225. - (Інформаційне забезпечення економічної безпеки підприємств та установ).
42. Щербина В. М. Актуальні проблеми економіки. - 2006. - № 10. - С. 220 - 225. - (Інформаційне забезпечення економічної безпеки підприємств та установ).
43. Ярочкин, В.И. Информационная безопасность.– М.: Академический Проект. Мир. 2014. – 544 с.
44. Software Engineering Institute Carnegie Mellon [Електронный ресурс] – Режим доступу до журн.: http://www.cert.org/octave/octaves.html.