Міністерство освіти і науки України
Західноукраїнський національний університет
Соціально-гуманітарний факультет
Кафедра інформаційної та соціокультурної діяльності

ТЕМА РОБОТИ:

Захист інформаційних ресурсів України

студентки 4 курсу ДІД-41 групи
Галузі знань 02 Культура і мистецтво
Спеціальності 029 «Інформаційна, бібліотечна, та архівна справа»
Кондратюк А.А
(прізвище та ініціали)

Керівник _____
_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Національна шкала _____
Кількість балів: _____ Оцінка: ECTS _____

Члени комісії _____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

Тернопіль – 2020

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 3
ВСТУП 4
РОЗДІЛ 1. ІНФОРМАЦІНІ РЕСУРСИ 5
1.1. Поняття інформаційних ресурсів 5
1.2. Правовий режим інформаційних ресурсів 8
РОЗДІЛ 2. ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ 12
2.1. Інформація та інформаційні системи підприємств 12
2.2. Організаційні заходи захисту інформації в інформаційних системах 15
РОЗДІЛ 3. ОБЛІК КОНФІДЕНЦІЙНИХ ДОКУМЕНТІВ 19
3.1. Документообіг як об’єкт захисту 19
3.2. Облік конфіденційних документів і формування довідково-інформаційного банку даних по документам 22
3.3. Перевірки наявності конфіденційних документів 25
ВИСНОВКИ 26
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 27

ВСТУП

Актуальність проблеми. У сучасному суспільстві інформація стає найбільш важливою цінністю, а індустрія отримання, обробки і захисту інформації – провідною галуззю діяльності, куди з кожним роком вкладають все більш значні капітали. Тому необхідно докласти зусиль у вирішенні питань стратегій і тактики розвитку системи інформаційної безпеки, що надавало б можливість захистити людину, суспільство, інформаційний простір тощо.

Аналіз останніх досліджень та наукових праць. Проведений аналіз нормативно-правового забезпечення захисту державних інформаційних ресурсів (ДІР) в інформаційній сфері нашого суспільства свідчить про малосистемний характер відповідної діяльності, спостерігається нечітка спрямованість визначення класів загроз різним видам ДІР (мало деталізовані, або відсутні).

Метою курсової роботи є дослідження організаційних заходів захисту інформаційних ресурсів України.

Відповідно до мети визначимо такі завдання:

- висвітлити – правовий режим інформаційних ресурсів;
- розкрити особливості – інформаційних систем підприємств;
- охарактеризувати – облік конфіденційних документів;
- проаналізувати – перевірки наявності конфіденційних документів;
- дати оцінку – організаційним заходам захисту інформації.

Об’єктом дослідження є захист інформаційних ресурсів України.

Предмет дослідження – інформація та інформаційні системи підприємств.

Курсова робота складається з вступу, трьох розділів та висновків. У вступі обґрунтована актуальність обраної теми дослідження. У першому розділі визначені теоретичні основи інформаційних ресурсів та правовий режим інформаційних ресурсів. Другий розділ курсової роботи відображає інформацію та інформаційні системи підприємств. У третьому розділі роботи окреслено заходи обліку конфіденційних документів.

РОЗДІЛ 1. ІНФОРМАЦІЙНІ РЕСУРСИ

1.1 Поняття інформаційних ресурсів

Загальне визначення інформаційного ресурсу міститься у ст. 1 Закону України «Про Національну програму інформатизації», де інформаційні ресурси визначаються як «сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо)».

У більш конкретному вигляді під інформаційними ресурсами розуміють організовану сукупність інформації, інформаційних продуктів та інформаційних технологій, які призначені для інформаційного забезпечення життєдіяльності людини, суспільства та держави. Тому, книги (найперші інформаційні ресурси), музеї, бібліотеки, архіви тощо – все це інформаційні ресурси.

Структуру інформаційних ресурсів складають масиви документів, окремі документи тощо, в яких накопичується та зберігається сформована за певними ознаками або критеріями інформація [1].

В науковій літературі пропонується безліч засад для класифікації інформаційних ресурсів.

Так, за природою інформації, яка їх створює, інформаційні ресурси поділяються на такі, що створюються зі штучної інформації та інформації, яка утворюється самостійно, незалежно від людини.

Перший клас інформаційних ресурсів створює інформація, яка утворюється самостійно. Наприклад, інформація про чисельність населення в країні, інформація гідрометцентру тощо.

До другого класу інформаційних ресурсів відноситься інформація, яка створюється штучно в результаті інтелектуальної діяльності людини. Наприклад, математична, логічна обробка інформації, літературні твори тощо. При цьому процес творчості припускає не тільки переробку вже відомої інформації, а й створення нової інформації – прогнозів, винаходів тощо.

За сферами використання інформаційні ресурси поділяються на бібліотеки, архіви, фонди інформації, електронні інформаційні системи тощо. В основі цієї класифікації лежать інтереси споживачів інформації. Споживач відноситься до інформації як до джерела своїх знань, яким він користується у повсякденному житті, під час отримання освіти, професійної підготовки, перепідготовки тощо. При цьому відбувається формування інформаційних ресурсів з урахуванням потреб споживачів [2].

За способам формування інформаційних масивів і розповсюдження інформації з них інформаційні ресурси поділяються на стаціонарні і мобільні.

Стаціонарні інформаційні ресурси формуються і використовуються, як правило, в спеціалізованих інформаційних організаціях за допомогою їх інформаційних систем і мереж, у том числі й через Інтернет. Основний механізм розповсюдження інформації з таких інформаційних ресурсів реалізується в порядку надання інформаційних послуг, тобто через пошук інформації в інформаційних системах цих організацій при зверненні до них користувачів (споживачів). Причому це може здійснюватися як безпосередньо самим користувачем, якщо такі можливості надаються йому відповідною інформаційною системою, так і через посередника. Споживач повинен знати місце розташування інформаційної організації і умови отримання інформації з її ресурсів. Такий механізм отримання інформації з інформаційного ресурсу заснований на принципі: споживач рухається до ресурсу.

Пересувні (або їх ще називають мобільними) інформаційні ресурси формуються державними і приватними (комерційними) інформаційними організаціями як спеціальні інформаційні продукти, головним чином, у вигляді банків даних. Такі інформаційні продукти тиражуються і розповсюджуються в комплексі – банк даних включає в свій склад і базу даних, і пошуковий апарат до неї. У цьому випадку, купуючи такий банк даних, споживач отримує можливість індивідуального користування ним на власному комп’ютері.

Отже, тут використовується принцип: ресурс «рухається» до споживача.

Інформаційні ресурси ще можна класифікувати за видами інформації, з якої вони складаються. З огляду на це існують інформаційні ресурси:

- правової інформації;
- науково-технічної інформації;
- політичної інформації;
- фінансово-економічної інформації;
- статистичної інформації;
- інформації про стандарти і регламенти, метрологічної інформації;
- соціальної інформації; інформації про охорону здоров'я; інформації про надзвичайні ситуації; персональної інформації (персональні дані); кадастри (земельний, містобудівний, майновий, лісний, інші);
- інформації іншого виду.

Інформаційні ресурси за способом доступу поділяються на інформаційні ресурси, які складаються з інформації відкритого доступу (без обмеження); інформації з обмеженим доступом (державна таємниця, конфіденційна інформація, комерційна таємниця, банківська та інші види таємниць, персональні дані).

За видом носія інформації інформаційні ресурси формуються на традиційному носії – папері, на комп'ютерних носіях інформації, в пам'яті комп'ютера, на сервері тощо.

За способом організації зберігання і використання інформаційні ресурси поділяються на традиційні (масив, фонд документів, архів) та автоматизовані (Інтернет, банк даних, автоматизована інформаційна система (мережа), база знань.

За формою власності інформаційні ресурси можуть мати статус загальноукраїнського національного надбання, державної власності, приватної власності, колективної власності [3].

1.2 Правовий режим інформаційних ресурсів

На законодавчому рівні України визначаються тільки інформаційні ресурси науково-технічної інформації та інформаційні ресурси спільного користування.

Згідно зі ст. 1 Закону України «Про науково-технічну інформацію»:

- під інформаційними ресурсами науково-технічної інформації розуміється систематизоване зібрання науково-технічної літератури і документації, зафіксоване на паперових чи інших носіях;

- під інформаційними ресурсами спільного користування розуміється сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових та науково-технічних бібліотек, центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання.

Об’єктом відносин у сфері науково-технічної інформації є документована на будь-яких носіях або публічно оголошувана вітчизняна або зарубіжна науково-технічна інформація.

За допомогою сучасних технологій, інформаційних систем, в тому числі автоматизованих, банків даних, мереж і, в першу, чергу Інтернет, сьогодні забезпечується реалізація процесу обігу інформації у суспільстві, формування інформаційних ресурсів, пошуку і розповсюдження інформації з них.

Суб’єктами відносин, що забезпечують реалізацію цих процесів є:

- громадяни, в тому числі іноземці, особи без громадянства; організації: бібліотеки; архіви; музеї;

- інформаційні центри й інші інформаційні структури, інформаційні фонди, центри аналізу інформації;

- інформаційні агентства, інші органи масової інформації;

- інші організації – власники інформаційних ресурсів;

- органи державної влади: Верховна Рада України, Президент України, Адміністрація Президента, Конституційний Суд, Верховний Суд, Кабінет Міністрів України, міністерства, відомства, комітети [4].

Власниками інформаційних ресурсів можуть бути як самостійні інформаційні центри, інформаційні організації, фірми, підприємства, установи, які мають статус юридичної особи (далі – інформаційні організації), так і окремі інформаційні структури (управління, відділи, лабораторії тощо) в складі інших юридичних осіб, а також фізичні особи.

Інформація з інформаційних ресурсів розповсюджується в результаті підготовки інформаційних продуктів і надання інформаційних послуг. Інформаційні продукти і інформаційні послуги також можна певним чином класифікувати.

Так, інформаційні продукти можуть бути у вигляді: документів, даних; добірок документів, даних; довідок, аналітичних довідок; баз даних, банків даних тощо.

Інформаційні послуги можна представити у вигляді послуг з інформаційного обслуговування: пошук інформації, обробка інформації, видача даних (документів), збереження інформації; послуги з користування Інтернет, автоматизованими інформаційними системами (далі АІС), банками даних, консультаційні послуги, послуги з передачі інформації, послуги з доступу до Інтернет, послуги з користування електронною поштою і формування особистих сайтів тощо.

Інформаційні продукти і послуги надаються споживачам відповідно до чинного законодавства, договору, запиту та ін. Споживач отримує їх у порядку самообслуговування, або через посередника. Інформація може надаватися як за плату (у тому числі - на пільгових основах), так і безкоштовно. Можливий також обмін інформацією.

При формуванні інформаційних ресурсів, підготовці і наданні користувачам інформаційних продуктів, інформаційних послуг, особливо при включенні таких ресурсів у транскордонні інформаційні мережі, в першу чергу Інтернет, необхідно вирішувати питання їх захисту від несанкціонованого доступу.

У зв’язку з цим повинні захищатися: інформаційні ресурси на всіх видах носіїв, у том числі ті, що містять інформацію обмеженого доступу; інформаційні

системи і їх мережі; інформаційні технології і засоби їх забезпечення; комп'ютерні носії з інформацією, наприклад, засобами електронного цифрового підпису чи криптографії; бази даних (знань) у складі автоматизованих інформаційних систем і їх мереж; програмні засоби, мережі тощо.

Особливу увагу необхідно приділяти формуванню і використанню державних інформаційних ресурсів в частині, що стосується забезпечення повноти і актуальності інформації, яку вони містять. Основна мета цієї роботи - максимально повне і відкрите надання інформації користувачам у порядку реалізації їх основного конституційного права на пошук і отримання достовірної та повної інформації.

Одним з видів сучасних інформаційних ресурсів є веб-ресурси. Веб-ресурси – це інформаційні ресурси у вигляді одного чи декількох веб-сайтів.

Веб-ресурси, як і будь-які інформаційні ресурси, можуть бути об'єктами усіх форм власності, договірних відносин згідно з цивільним законодавством та законодавством про інтелектуальну власність.

Згідно з законодавством, веб-сайти загального інформаційного змісту не повинні містити персональні дані або інформацію, що становить державну таємницю, та іншу інформацію, що обмежена у поширенні.

При розміщенні інформації на веб-ресурсі власник повинен:

- не розміщувати на своєму веб-сайті інформацію насильницького, фашистського або іншого антилюдського змісту;
- поважати релігійні, національні, культурні, політичні, професійні та інші права громадян, не розповсюджувати інформацію, яка може спровокувати національну або релігійну ворожнечу;
- не розміщувати інформацію, що може зашкодити честі, гідності та репутації окремих осіб;
- не розголошувати конфіденційну інформацію, а також персональні дані без згоди на це суб'єкту даних;
- дотримуватись норм культури і моралі та інше.

Забороняється використання веб-ресурсів для:

- втручання в особисте життя громадян;
- розміщення персональних даних в базах даних загального інформаційного призначення;
- поширення спотвореної інформації.

Власник інформації, у випадку нанесення йому моральної чи матеріальної шкоди в результаті поширення інформації на веб-сайті має право на повне відшкодування, згідно з чинним законодавством України на підставі рішення суду.

Власник веб-ресурсу може зареєструвати належний йому інформаційний ресурс як засіб масової інформації, що поширює відомості у телекомунікаційних мережах, у випадку, коли метою створення цього ресурсу або змістом його діяльності є розповсюдження масової інформації [5].

РОЗДІЛ 2. ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ПІДПРИЄМСТВ

2.1 Інформація та інформаційні системи підприємств

Інформація та інформаційні системи (інформаційні системи – далі ІС) підприємств, мережеве оточення, у яких вони функціонують, є невід'ємними складовими сучасного бізнес-середовища. Їх доступність, цілісність і конфіденційність можуть мати вирішальне значення для забезпечення конкурентоспроможності підприємства, руху коштів, рентабельності, відповідності правовим нормам і стандартам. Водночас, унаслідок посилення залежності підприємств від інформаційних, комунікаційних систем і сервісів вони стають вразливішими до порушень режиму безпеки. Поширення інформаційних і комунікаційних систем надає все нові можливості несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи обмежує можливості фахівців централізовано контролювати ІС та мережеве оточення [6].

Порушення режиму безпеки ІС може істотно ускладнити реалізацію виробничих завдань, тому вирішення проблеми формування ефективної системи захисту інформації (захист інформації – далі ЗІ) набуває дуже важливого значення. Це пояснюється тим, що у процесах розроблення й удосконалення систем ЗІ є чимало недостатньо вивчених і досліджених аспектів, які можуть негативно впливати на показники ефективності та надійності функціонування системи безпеки загалом.

Вимогою сьогодення є необхідність вирішення питань фізичної безпеки, управління інцидентами, виконання законодавчих актів, стандартів, настанов.

Аналіз наукових публікацій дає підстави стверджувати, що у процесі проектування, створення й експлуатування систем ЗІ трапляються помилки та недоречності, які суттєво знижують ефективність їх функціонування. Вимагає окремого обґрунтування розроблення політики інформаційної безпеки, яка

визначає стратегію і тактику системи ЗІ в ІС підприємств і враховує динаміку процесів зміни типів і рівня загроз інформації, що є одним з активних і значущих ресурсів сучасного бізнес-середовища.

Система ЗІ в ІС підприємств повинна будуватися на засадах комплексності й адаптивності. Доцільно розробляти організаційну структуру і впроваджувати систему ЗІ в ІС підприємств відповідно до рекомендацій міжнародних стандартів і чинного законодавства України. Дотримання принципів стандартів серії ISO 27000 забезпечує керування і контроль за доступом, розробкою й обслуговуванням апаратно-програмних систем, керування безперервністю бізнес-процесів. Відповідність вимогам ISO 27000 і дотримання національних правових норм з інформаційної безпеки є необхідними для сталого розвитку бізнесу [7].

Метою дослідження є визначення методів і засобів ЗІ в ІС підприємств. Пропонується використовувати набір організаційно-технічних методів і засобів, які дозволяють формувати ефективні системи ЗІ. Відзначимо, що ці методи є лише одним з аспектів реалізації цілісної концепції управління інформаційною безпекою ІС підприємства.

У публікації не розглядаються методи ЗІ, які ґрунтуються на системному адмініструванні та спеціальних математичних методах і алгоритмах. Основна увага зосереджена на розробці й аналізі організаційно-технічних заходів, які будуть зрозумілими і для менеджменту середньої ланки, і для керівництва підприємства.

Основні результати дослідження. Законодавчі заходи щодо ЗІ полягають у виконанні чинних у державі або введенні нових законів, нормативних документів, настанов, що регулюють правову відповідальність посадових осіб за втрату або зміну інформації, що підлягає захисту, зокрема, за спроби виконувати аналогічні дії за межами своїх повноважень, а також відповідальність сторонніх осіб за спробу несанкціонованого доступу до інформації. Мета правових заходів полягає у запобіганні можливим правопорушенням і встановленні відповідальності за здійснені правопорушення.

Правову основу у вирішенні проблем ЗІ в Україні формують Конституція України, Закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні угоди України з питань технічного захисту інформації, згода на обов'язковість яких надана Верховною Радою України. В Україні діє близько 60 нормативних актів, які безпосередньо або опосередковано стосуються регулювання відносин у інформаційній сфері. Окрім цього, діє низка відомчих актів, тлумачень, методик, які є обов'язковими для виконання всіма державними органами, підприємствами, установами, організаціями під час виконання функцій із забезпечення захисту інформації з обмеженим доступом (інформація з обмеженим доступом – далі ІзОД), насамперед, це стосується державної таємниці [8].

Регулятивно-правову основу забезпечення ЗІ в ІС підприємств України різної форми власності становлять: Конституція України; Концепція національної безпеки України; Закони України: «Про державну таємницю»; «Про доступ до публічної інформації; «Про інформацію»; «Про науково-технічну інформацію».

Впровадження та дотримання вимог стандартів з питань ЗІ не може трактуватися як одномоментна, разова акція. Це, фактично, є безперервним процесом розробки, впровадження, функціонування, моніторингу, перегляду, підтримки та вдосконалення цілісної системи інформаційної безпеки як складової частини ІС підприємств.

2.2 Організаційні заходи захисту інформації в інформаційних системах

З метою протидії процесам неконтрольованого витоку, несанкціонованого доступу (несанкціонований доступ – далі НСД), модифікування службової інформації та зменшення збитків від реалізація цих загроз потрібно фахово формувати заходи і вибирати засоби забезпечення ЗІ. Необхідно також володіти знаннями основних правових положень у цій галузі, вміти ефективно реалізовувати організаційні, програмнотехнічні та інші заходи із забезпечення безпеки інформації.

Актуальність вирішення даної проблеми пов’язана із суттєвим зростанням можливостей сучасних інформаційних технологій (ІТ). Розвиток програмно-апаратних засобів, методів і способів обробки інформації та широке застосування ІТ роблять інформацію більш уразливою.

Процедура проектування системи ЗІ та вибору засобів ЗІ в ІС є складним комплексним завданням, при вирішенні якого потрібно враховувати різні типи ймовірних загроз для безпечного функціонування ІС, вартість реалізації ЗІ і наявність численних зацікавлених сторін.

При забезпеченні ЗІ основним елементом є процедура аналізу можливих загроз функціонуванню ІС, тобто загроз, що підвищують уразливість інформації, яка обробляється ІС, призводять до її неконтрольованого витоку, випадкового або цілеспрямованого модифікування, знищення.

Засоби системи ЗІ не варто проектувати, закуповувати або встановлювати доти, поки не буде виконаний аналіз ризиків та імовірних загроз. Тільки ґрунтовний аналіз ризиків і загроз дає об’єктивну оцінку наслідків реалізації загроз, збитків від комерційних втрат, зниження коефіцієнта готовності системи ЗІ, правових проблем, інформацію для визначення найпридатніших методів і засобів забезпечення належного рівня безпеки ІС підприємств [9].

Розглядаючи загальні засади ЗІ в ІС, доцільно відзначити, що комплексний ЗІ в ІС передбачає використання спеціальних правових, фізичних, організаційних

і програмно-апаратних засобів ЗІ, які повинні забезпечувати ідентифікацію й аутентифікацію користувачів, розподіл повноважень доступу до технічних, інформаційних ресурсів і сервісів ІС, реєстрування та облік спроб НСД.

Організаційні заходи ЗІ в ІС, як правило, спрямовані на чіткий розподіл відповідальності персоналу в процесах опрацювання інформації, створення декількох рубежів контролю, запобігання зовнішнім та інсайдерським загрозам, навмисному або випадковому знищенню й модифікуванню інформації.

Об’єктом технічного захисту, відповідно до чинного законодавства, є інформація, яка становить державну або іншу, передбачену чинним законодавством України, таємницю, службова інформація, яка є державною власністю або передана державі у володіння, користування, розпорядження.

Технічний захист інформації (технічний захист інформації – далі ТЗІ) здійснюється у кілька етапів: перший етап – визначення і аналіз загроз; другий етап – розробка системи ЗІ; третій етап – реалізація плану ЗІ; четвертий етап – контроль за функціонуванням і керуванням системою ЗІ.

На першому етапі здійснюється ґрунтовний аналіз об’єктів ТЗІ, ситуаційного плану, умов функціонування ІС, оцінювання ймовірності прояву загроз та очікувані збитки від їх реалізація, підготовка даних для побудови моделі загроз.

Загрози можуть здійснюватися:

- технічними каналами, які включають канали побічних електромагнітних випромінювань і наведень, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи ЗІ або порушення цілісності інформації;

- НСД шляхом під’єднання до апаратури та ліній зв’язку, маскуванням під зареєстрованого користувача, подоланням заходів захисту Web-ресурсів, застосуванням закладних пристроїв, програм і вкоріненням комп’ютерних вірусів.

На другому етапі ТЗІ розробляється план, який містить організаційні, первинні технічні й основні технічні заходи захисту ІзОД, визначаються зони

безпеки інформації. Організаційні заходи регламентують порядок інформаційної діяльності (інформаційна діяльність – далі ІД) з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу ІД.

Первинні технічні заходи передбачають ЗІ блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають ЗІ з використанням засобів ТЗІ. Заходи захисту інформації повинні:

- бути адекватними до загроз;

- бути розробленими з урахуванням можливих збитків від реалізація загроз і вартості захисних заходів та обмежень, які вносяться ними;

- забезпечувати задану ефективність ЗІ на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Мінімально необхідний рівень ЗІ забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

На третьому етапі ТЗІ слід реалізувати організаційні, первинні технічні й основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестування технічних засобів забезпечення інформаційної діяльності (ІД) підприємств, технічних засобів ЗІ, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

ТЗІ передбачає застосування захищених програм і технічних засобів забезпечення ІД, програмних і технічних засобів ЗІ та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем.

На четвертому етапі здійснюється контроль за функціонуванням та управлінням системою ТЗІ на об’єктах ІД з метою визначення й удосконалення стану ЗІ в ІС, виявлення та запобігання порушенням системи ЗІ. Контроль стану ЗІ в ІС організовується відповідно до планів, затверджених керівниками підприємств, шляхом проведення перевірок.

Контрольно-інспекційна робота з питань ЗІ включає планування та проведення перевірок стану ЗІ в ІС, щодо яких здійснюється ТЗІ, проведення аналізу та надання настанов з удосконалення заходів щодо ТЗІ.

Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

Під час комплексної перевірки вивчається й оцінюється стан ЗІ в ІС, щодо яких здійснюється ТЗІ.

Під час цільової (тематичної) перевірки вивчаються окремі напрямки ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ЗІ в ІС, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності у галузі ТЗІ за відповідними дозволами та ліцензіями суб'єктами системи ЗІ.

Під час контрольної перевірки перевіряється усунення недоліків, які були виявлені попередньою комплексною або цільовою перевіркою. Відзначені перевірки можуть бути планові та позапланові, з попередженням та раптові.

Позапланова перевірка здійснюється за вказівкою вищого менеджменту підприємства у разі виникнення потреби визначення повноти та достатності заходів щодо ТЗІ за наявності відомостей про порушення виконання вимог нормативно-правових актів з питань ЗІ.

Перевірки здійснюються комісіями, на які покладено виконання завдань здійснення контролю за функціонуванням системи ЗІ. При проведенні перевірки стану ЗІ контролю підлягають організаційні, організаційно-технічні, технічні заходи ЗІ у виділених приміщеннях, ІС і периметру корпоративної мережі, повнота та достатність робіт з атестування виділених приміщень [10].

РОЗДІЛ 3. ОБЛІК КОФІДЕНЦІЙНИХ ДОКУМЕНТІВ

3.1 Документообіг як об’єкт захисту

Головною метою обліку конфіденційних документів є, насамперед, формування інформаційної бази, що забезпечує постійне пильнування за збереженням кожного документу і своєчасне фіксування його місцезнаходження.

Документообіг як об’єкт захисту представляє собою сукупність (мережу) каналів розповсюдження документованої конфіденційної інформації по споживачам у процесі управлінської та виробничої діяльності. Рух документованої інформації не можна розпродати тільки як механічне переміщення документів по інстанціям, як функцію поштової доставки кореспонденції адресатам.

Основною характеристикою такого руху є його технологічна комплексність, тобто з’єднання в єдине ціле управлінських, діловодних та поштових задач, що визначають в сукупності зміст переміщення документів. При русі документів (в тому числі електронних) по інстанціях створюються потенційні можливості втрати цієї інформації за рахунок розширення числа джерел, що володіють цінною інформацією [11].

Загрози документам в документопотоках включають в себе:

- викрадення, загублення документу або його окремих частіш (додатків, примірників, листів, вклейок, вставок, чорновиків, редакцій і ті);

- копіювання паперових і електронних документів, фото-, відео-, аудіодокументів і баз даних;

- підміну документів, носіїв і їх окремих частин з метою фальсифікації або приховування факту загублення, викрадення;

- таємне чи дозволене ознайомлення з документами і базами даних, запам’ятовування і переказ інформації зловмиснику;

- дистанційний перегляд документів і зображення дисплея за допомогою спеціальних технічних засобів;

- помилкові дії персоналу під час роботи з документами (порушення дозвільної системи, порядку обробки документів, правил роботи з документами і т. д.);

- випадкове або зловмисне знищення цінних документів і баз даних, їх несанкціонована модифікація, спотворення і фальсифікація, зчитування даних в чужих масивах за рахунок роботи з залишковою інформацією на копіювальній стрічці, папері, дискам ЕОМ;

- маскування під зареєстрованого користувача;

- витік інформації по технічним каналам під час обговорення і диктування тексту документа, виготовлення документів. Головним напрямом захисту документованої інформації (документів) від всіх видів загроз є формування захищеного документообігу і використання в обробці і зберіганій, документів технологічної системи, що забезпечує безпеку інформації на любому типі носія. За рахунок цього досягається можливість контролю конфіденційної інформації в її джерелах і каналах розповсюдження. Окрім загальних для документообігу принципів захищений документообіг базується на ряді додаткових принципів:

- персональної відповідальності співробітників за збереження носія і таємницю інформації;

- обмеженні ділової необхідності доступу персоналу до документів, справ і базам даних;

- операційному обліку документів і контролю за їх збереженням у процесі руху, розгляду, виконання і використання;

- жорсткій регламентації порядку роботи з документами, справами і базами даних для всіх категорій персоналу. В великих підприємницьких структурах з великим об’ємом документів в потоках захищеність документообігу досягається за рахунок:

- формування самостійних, ізольованих потоків конфіденційних (грифованих) документів і, часто, додаткового дроблення їх на ізольовані потоки у відповідності з рівнем конфіденційності (рівнем грифу) документів, що переміщаються;

- використання централізованої автономної технологічної системи обробки і зберігання конфіденційних документів, ізольованої від системи обробки інших документів;

- організації самостійного підрозділу (служби) конфіденційної документації або аналогічного підрозділу, що входить у склад служби безпеки, аналітичної служби фірми.

В підприємницьких структурах з невеликим складом штатних співробітників та об'ємом опрацьованих документів (наприклад, в малому бізнесі), а також в структурах, основна маса документів в яких є конфіденційною (наприклад, в банках, страхових компаніях), конфіденційні документи можуть не виділятися з загального документопотоку і оброблятися в рамках єдиної технологічної системи.

Підрозділ конфіденційної документації в таких підприємницьких структурах зазвичай не створюється. Функції централізованої обробки і зберігання конфіденційних документів покладаються на керуючого справами, референта або інколи досвідченого секретаря-референта фірми. При любому варіанті побудови захищеного документообігу вжиті для безпеки інформації міри не повинні збільшувати терміни руху та виконання документів [12].

Однією з найважливіших вимог до захищеного документообігу є вибірковість у доставці і використання персоналом цінної інформації. Вибірковість призначена не тільки для забезпечення оперативності в отримання користувачем цінної інформації, але й обмеження у доставці йому тієї інформації, робота з якою йому дозволена у відповідності з його функціональними обов'язками.

3.2 Облік конфіденційних документів і формування довідково-інформаційного банку даних по документам

Облік конфіденційних документів передбачає не тільки реєстрацію факсу створення (видання) або отримання документа, але й обов'язково фіксацію зсік переміщень документа по інстанціях, керівникам і виконавцям у процесі розгляду, виконання і використання документів.

Облік цих документів та їх зберігання завжди централізовані в підрозділі конфіденційної документації фірми або у референта першого керівника. Голосною метою обліку конфіденційних документів є забезпечення їх фізичного збереження [13].

Облік конфіденційних документів вирішує наступні завдання:

– фіксування факту надходження або видання документа;

– фіксування місця знаходження документа;

– забезпечення пошуку документів під час перевірив наявності або необхідності звернення до документу;

– забезпечення довідково-інформаційної і контрольної роботи по документах;

– попередження втрати копій та примірників документу, чорновиків і редакцій, додатків та окремих листків. Для вирішення. цих завдань доцільно вести наступні види обліку конфіденційних документів фірми:

– облік вхідних документів;

– облік підготовлених, виданих вихідних (ті, що відправляються) і внутрішніх документів;

– інвентарний (виділений) облік документів, справ та носіїв конфіденційної інформації.

При любому виді обліку індексування конфіденційних документів базується на валовій нумерації документів всього потоку на протязі календарного року. Перевага валової нумерації по лягає в гарантованому збереженні номеру,

виділеного для даного документу, записі вихідних відомостей про документ і картку, заведену на документ.

Ні один номер не може щезнути, а карточка випасти із систематизованого по номерам масиву. Серйозним недоліком валової нумерації документів є відсутність її прив'язки до місця зберігання документу.

Кожній запис завіряється розписами співробітники служби конфіденційної документації і виконавця або другого співробітника цієї служби. При заповненні на конфіденційних документ одного примірника облікової картки виникає необхідність ведення контрольного журналу [14].

Журнал призначеній для забезпечення послідовності присвоєння документам порядкових облікових номерів, контролю за наявністю документів і карток, прискорення пошуку документів. Напроти облікового номеру документу в журналі зазначається прізвище особи, яка розписалася в картці за отримання документу, тобто фіксується місцезнаходження документу.

Традиційний обліковий та довідково-інформаційний банк даних по конфіденційним документам звичайно включає в себе:

- довідкову картотеку на невиконані документи, в якій перші примірники карток розташовуються по виконавцям;
- валову картотеку з розділами невиконаних (для других примірників карток) і виконаних (дня перших примірників карток) документів, в якій картки розташовуються в послідовності облікових номерів документів;
- контрольну картотеку, в якій додаткові примірники карток розташовуються по термінам виконання документів;
- довідкову картотеку на виконані документи, в якій другі примірники карток розташовуються по кореспондентам.

Якщо на конфіденційні документи ведеться довідкова картотека, аналогічна картотеці на відкриті документи, то частина картотеки на невиконані документи формується по виконавцям, а в частині на виконані документи картки розташовуються по рубрикам номенклатури справ (якщо нумерація документів

ведеться по кожній справі окремо) або у валовій послідовності номерів документів [15].

Автоматизований довідково-інформаційний банк даних по конфіденційних документах має допоміжне значення і ведеться разом з банком даних на паперових носіях. Автоматизований банк даних реалізує функцію довідкового та пошукового обслуговування користувачів, контролю виконання документів і інколи роботи персоналу з електронними аналогами паперових документів.

Облікова функція зберігається за традиційним банком даних. Відомості про зміну місцезнаходження документа вносяться в електронний журнал, який виконує в даному випадку роль контрольного журналу.

Після виконання робиться нова роздруківка повних відомостей про документ, яка розміщується в традиційну картотеку замість роздруківки вихідних відомостей про документ, яка там знаходилась. Видача документів виконавцям здійснюється по роздруківкам облікового журналу (карток обліку) документів, в яких фіксується розпис за отримання і повернення документів.

Документи (наприклад, інвентарного обліку) можуть також видаватися під розпис в роздруківці картки обліку видачі документа. У великих підприємницьких структурах інколи використовується метод "електронного підпису" за отримання і повернення електронного документу. Подібна автоматизовані системи повинні базуватися на чітких принципах і методах розмежування доступу до інформації, мати комплексний захист від зловмисника [16].

3.3 Перевірки наявності конфіденційних документів

Облік конфіденційних документів дозволяє не тільки забезпечити збереження документів і організувати по ним довідково-інформаційну і контрольну роботу, але й проводити періодичні і неперіодичні перевірки наявності документів.

Метою перевірки наявності конфіденційних документів є встановлення фактичної відповідності наявних документів записам в облікових формах, їх збереженню, цілісності і комплектності. Такі перевірки спонукають виконавців до ретельного дотримання правил роботи з документами і піклування про їх фізичне збереження [17].

Перевірка проводиться від облікових даних до документів, примірникам документів і складовим частинам кожного примірника.

Регламентовані, обов’язкові перевірки наявності конфіденційних документів проводяться щоквартально і по закінченні календарного року. Не регламентовані перевірки здійснюються при зміні керівництва підрозділів, звільненні виконавця, після закінчення екстремальної ситуації, виявлення фактів загрози інформації і в інших випадках. Якщо регламентовані перевірки наявності охоплюють всі конфіденційні документи фірми, то при нерегламентованій перевірці обмежуються конкретною частішою документації [18].

Перевірки наявності документів проводяться спеціально призначеною комісією, в яку звичайно входять:

- заступник керівника фірми,
- керівник служби безпеки та інші особи.

По результатам перевірки складається акт. Щоденні перевірки наявності документів (самоперевірки) проводяться по закінченні робочого дня всіма співробітниками, що працюють з конфіденційними документами.

ВИСНОВКИ

Вищевикладене дає підстави стверджувати, що система захисту інформації в інформаційних системах підприємств повинна будуватися на засадах комплексності й адаптивності. Контроль за реалізацією організаційно-технічних заходів щодо технічного захисту інформації у виділених приміщеннях, інформаційних систем та корпоративних мереж, повнотою та достатністю робіт з атестування виділених приміщень повинен включати перевірку відповідності виконання цих заходів вимогам чинного законодавства України, нормативно-правових актів з питань захисту інформації.

Організаційно-технічні заходи технічного захисту інформації у виділених приміщеннях, ІС та периметру корпоративних мереж, роботи з атестування виділених приміщень виконуються власними силами або передаються на аутсорсинг суб'єктам підприємницької діяльності у галузі захисту інформації, які мають дозвіл і ліцензію від уповноваженого Кабінетом Міністрів України органу.

Керівник підприємства зобов'язаний вжити невідкладних заходів з усунення недоліків і реалізації пропозицій комісії відповідно до вимог нормативно-правових актів з питань захисту інформації.

Розглядаючи розділ обліку конфіденційних документів, зрозуміли що головною метою обліку конфіденційних документів є, насамперед, формування інформаційної бази, що забезпечує постійне пильнування за збереженням кожного документу і своєчасне фіксування його місцезнаходження.

Облік конфіденційних документів дозволяє не тільки забезпечити збереження документів і організувати по ним довідково-інформаційну і контрольну роботу, але й проводити періодичні і неперіодичні перевірки наявності документів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію: Закон України від 02 жовтня 1992 р. // Відомості Верховної Ради України. - 1992. - № 48. Ст. 651.

2. Про Національну програму інформатизації: Закон України від 4 лютого 1998 р. // Відомості Верховної Ради України. – 2002. - № 1. Ст. 3.

3. Про науково-технічну інформацію: Закон України відвід 20 листопада 2003 року№ 1294-IV.

4. Копылов В.А. Информационное право: Учебник. - 2-е изд., перераб. и доп. - М.: Юристь, 2002.

5. Конституція України // zakon.rada.gov.ua.

6. Про державну таємницю: Закон України від 21.01.1994 №3855-XII // zakon.rada.gov.ua.

7. Про доступ до публічної інформації: Закон України від 13.01.2011 №2939-VI // zakon.rada. gov.ua.

8. Про інформацію: Закон України від 02.10.1992 №2657-XII // zakon.rada.gov.ua.

9. Про науково-технічну інформацію: Закон України від 25.06.1993 №3322-XII // zakon. rada.gov.ua.

10. Про Концепцію національної безпеки України: Постанова Верховної Ради України від 16.01.1997 №3/97-ВР // zakon.rada.gov.ua.

11. Гарасимчук О.І., Дудикевич В.Б., Ромака В.А. Комплексні системи санкціонованого доступу: Навч. посібник. – Львів: Львівська політехніка, 2010. – 212 с.

12. Когут В.В., Рудий Т.В., Кулешник Я.Ф. Порядок атестування систем технічного захисту інформації // Проблеми діяльності кримінальної міліції в умовах розбудови правової держави: Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ (12 березня 2010 р.). – Львів: ЛьвДУВС, 2010. – С. 90–97.

13. Кохановська О.В. Правове регулювання у сфері інформаційних відносин.-К.:НАВСУ, 2001.

14. Правова інформатика: (системна інформатизація законотворчої, правозастосовної, правоохоронної, судочинної та правоосвітньої діяльності в Україні): Монографія / М.Я. Швець, Р.А. Калюжний, В.А. Саницький та ін.; За ред. М.Я. Швеця, Р.А. Калюжного. – Ужгород: ІВА, 2003. – 168 с.

15. Основи інформаційного права України: Навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.В. Грищенко та ін.; За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника – К.: Знання, 2004. – 274 с.

16. Хахановський В.Г., Мартиненко І.В. Смаглюк В.М., Інформаційне право та правова інформатика: навчальна програма (спеціальність 7.060101 – правознавство). - К.: НАВСУ, 2004.

17. Хахановський В.Г., Мартиненко І.В. Смаглюк В.М., Інформаційне право та правова інформатика: навчально-методичний комплекс (спеціальність 7.060101 – правознавство для студентів Юридичного факультету).- К.: НАВСУ, 2004.

18. Шеннон К. Работа по теории информации и кибернетике. – М.: Из-во иностранной литературы, 1963. – 829 с.