Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: «*Захист інформації в автоматизованій системі адвокатського об'єднання "Захист права"*»

Виконав(ла): студент(ка) VI курсу, групи СБм-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

		Забавчук І.І.
	(підпис)	(прізвище та ініціали)
Керівник		Марценюк В.П.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Кареліна О.В.
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Загородна Н.В.
	(підпис)	(прізвище та ініціали)
Рецензент		Матійчук Л.П.
	(підпис)	(прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

Факультет Комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпека
(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_________ Загородна Н. В.
(підпис) (прізвище та ініціали)

« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 «Кібербезпека»
(шифр і назва спеціальності)

студенту Забавчуку Ігорю Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Захист інформації в автоматизованій системі адвокатського об'єднання "Захист права"

Керівник роботи Марценюк Василь Петрович д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «09» листопада 2021 року № 4/7-941

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ 1. Розд. 1.1 Історіографія та методика дослідження КСЗІ
Розд. 1.2 Комплексна система захисту інформації: поняття та структура
Розд. 1.3 Побудова КСЗІ адвокатського об'єднання „Захист права" з урахуванням міжнародних стандартів
4 Охорона праці та безпека в надзвичайних ситуаціях. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1 Захист інформації в автоматизованій системі адвокатського об'єднання „Захист права" 2 Мета роботи, Задачі, об'єкт дослідження, предмет дослідження, наукова новизна. 3 Класифікація інформації 4 Складові КСЗІ
5 Етапи створення КСЗІ, 6 План адвокатської організації „Захист права" 7 Межі контрольованої зони [illegible] відомостей, що відносяться до конфіденційної інформації, адвокатська таємниця [illegible]
[illegible] класифікація порушників 9 класифікація загроз [illegible]

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата: завдання видав	Підпис, дата: завдання прийняв
Безпека в надзвичайних ситуаціях	Клепчик В.М.	[illegible]	[illegible]
Охорона праці	Осухівська Г.М.		

7. Дата видачі завдання ____________

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Прим…
1	Отримання завдання і аналіз теми	20.09.2021	Викон…
2	Ознайомлення з принципами, способами та методами захисту інформації в автоматизованих системах	24.09.2021	Викон…
3	Аналіз середовища ІТС	11.10.2021	Викон…
4	Формування моделі загроз і моделі порушника	28.10.2021	Викон…
5	Побудова КСЗІ для автоматизованої системи	15.11.2021	Викон…
6	Охорона праці та безпека у надзвичайних ситуаціях	29.11.2021	Викон…
7	Оформлення кваліфікаційної роботи	10.12.2021	Викон…
8	Перевірка роботи на антиплагіат	19.12.2021	Викон…
9	Попередній захист роботи	20.12.2021	Викон…
10	Захист кваліфікаційної роботи	23.12.2021	

Студент ____________ (підпис) ____________ Забавчук І.І. (прізвище та ініціали)

Керівник роботи ____________ (підпис) ____________ Марценюк В.П. (прізвище та ініціали)

АНОТАЦІЯ

Захист інформації в автоматизованій системі адвокатського об’єднання «Захист права» // Дипломна робота ОР «Магістр» // Забавчук Ігор Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-61 // Тернопіль, 2021 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: ІНФОРМАЦІЯ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, АДВОКАТСЬКА ТАЄМНИЦЯ, КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ.

У даній дипломній роботі розглянуті питання, пов'язані з впровадженням захисту цифрової інформації в адвокатській діяльності. В ході виконання роботи проведено аналіз доцільності захисту адвокатської таємниці в автоматизованих системах.

У першому розділі дипломної роботи розглянута історіографія і методологія захисту інформації в інформаційних системах з урахуванням специфіки адвокатської діяльності.

У другому розділі дипломної роботи представлено елементи структури КСЗІ в адвокатському об’єднанні. Проаналізовано вимоги щодо впровадження системи ТЗІ для адвокатської діяльності.

У третьому розділі дослідження класифіковано інформацію, яка підлягає захисту в адвокатському об’єднанні. Проведено аналіз видів інформації в адвокатській діяльності та структурований підхід, який проявив себе у поглинанні певних видів інформації адвокатською таємницею.

Прийшли до висновків, що адвокатська таємниця включає в себе конфіденційну інформацію та в окремих випадках комерційну таємницю. Вважаємо за необхідне внести зміни до нормативних документів з питань захисту інформації щодо відображення адвокатської таємниці в окремий вид, де включити вимоги щодо створення системи технічного захисту інформації.

ANNOTATION

Information protection in an automated system of the lawyers' association "Zakhyst prava" // Final thesis of educational level "Master" // Zabavchuk Igor Igorovych // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2021 // P. , Fig. – , Tables – , Annexes – , References. – .

Key words: INFORMATION, COMPREHENSIVE CASE INFORMATION PROTECTION SYSTEM, LAWYER SECRET, CONFIDENTIAL INFORMATION.

This thesis discusses issues related to the introduction of digital information protection in advocacy. While conducting thesis the analysis of expediency of protection of lawyer's secret in automated systems was carried out.

In the first section of the thesis the historiography and methodology of information protection in information systems taking into account the specifics of advocacy are considered.

The second section of the thesis presents the elements of the structure of the Comprehensive Case Information System in the advocacy association. The requirements for the implementation of the TSI system for advocacy are analyzed.

The third section of the study classifies information that is subject to protection by a law firm. An analysis of the types of information in advocacy and a structured approach that has manifested itself in the absorption of certain types of information by advocacy.

It was concluded that legal secrecy includes confidential information and in some cases trade secrets. We consider it necessary to make changes to the regulations on the protection of information on the disclosure of legal secrecy in a separate form, which includes requirements for the establishment of a system of technical protection of information.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС – автоматизована система;

АСЕ – автоматизована система управління;

АСНД – автоматизована система наукових досліджень;

ДТЗС – додаткові технічні засоби та системи;

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації України;

ЗОТ – засіб обчислювальної техніки;

ІзОД – інформація з обмеженим доступом;

КЗЗ – комплекс засобів захисту від несанкціонованого доступу;

КТ – контрольована територія;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОС – операційна система;

ОТЗС – основні технічні засоби та системи;

ПЗ – програмне забезпечення;

СУІБ – система управління інформаційною безпекою;

ТЗ – технічне завдання;

ФПЗ – функціональні послуги захисту.

ВСТУП

Розвиток інформаційних технологій віднайшов свій відбиток в усіх сферах нашого життя. Відповідно безпека інформаційних ресурсів є ключовою проблемою сьогодення.

Не обійшов стороною цей процес і адвокатську діяльність, зокрема і в нашій державі. Важко тепер уявити адвоката, який не використовує інформаційні технології у своїй практиці.

Одним з головним завдань для адвоката, окрім належного захисту клієнта, є збереження адвокатської таємниці. Однак, головний акцент чомусь зумовлений саме на усне збереження таємниці чи відображеної на паперових носіях, незважаючи на той факт, що значні масиви інформації формуються першочергово в електронному вигляді.

Саме тому, захист цифрової інформації, яка циркулює в адвокатських об’єднаннях є досить актуальним завданням на сьогоднішній день.

В нашій роботі представлено один з варіантів захисту адвокатської таємниці шляхом впровадження комплексної системи захисту інформації на базі Адвокатського об’єднання «Захист права».

Актуальність дослідження зумовлена тим, що робота є першим науковим пошуком розв’язання проблем захисту адвокатської таємниці в АС. Підлягають вирішенню питання класифікації інформації, яка входить до адвокатської таємниці в залежності від наявної нормативної бази.

Метою роботи є впровадження головних елементів захисту цифрової інформації, яка використовується в адвокатській діяльності.

Об’єктом дослідження є сфера захисту інформації в інформаційно-телекомунікаційних системах.

Предметом дослідження є захист інформації в автоматизованій системі адвокатського об’єднання «Захист права».

Для досягнення поставленої мети вирішенню підлягають такі завдання:

1) охарактеризувати історіографію та методологію захисту інформації ІТС з урахуванням адвокатської діяльності;

2) сформувати загальні вимоги та розробити політику безпеки КСЗІ на базі адвокатського об’єднання;

3) класифікувати інформацію, яка підлягає захисту в адвокатському об’єднанні.

РОЗДІЛ 1 ІСТОРІОГРАФІЯ ТА МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ КСЗІ

1.1 Історіографія дослідження КСЗІ в контексті розвитку адвокатського самоврядування

На початку 1970-х років проблеми безпеки інформації тільки починали опрацьовуватися, спроби пов'язати роботу комп'ютерних систем з існуючими системами класифікації секретної інформації. На практиці це породжувало складні проблеми. Одна полягала в тому, що ЕОМ і ОС влаштовані складно, що для розуміння програмісти або оператори могли закладати в них будь-які документовані функції, без ризику бути виявленими. Інша велика проблема була в розподіленні ресурсів однієї ЕОМ на роботу з будь-якими рівнями секретності, тобто люди з різними формами допуску взаємодіяли з одним фізичним сховищем.

В цей час питання щодо захисту адвокатської таємниці в автоматизованих системах не виникали, оскільки ЕОМ застосовувалися виключно в спеціальних галузях господарства, космічній, оборонній тощо.

Є думка, що проблеми інформаційного захисту стосуються безпосередньо інформації, що обробляється комп'ютером. Це, мабуть, стосується того, що комп'ютер і, зокрема, персональний комп'ютер являється «ядром», центром зберігання інформації. Інформаційний об'єкт, стосовно до якого спрямовані дії інформаційного захисту, видається широким поняттям у порівнянні з персональним комп'ютером[1, с. 1].

У реальному житті “об'єкти інформатизації” розміщені в межах одного підприємства і є єдиний комплекс компонентів, пов'язані метою, завданнями, структурними відносинами, технологією обміну інформації і т. д.

Сучасне підприємство є складною системою яка об’єднує багато різноманітних компонентів, які виконують визначені цілі та в процесі

функціонування підприємства можуть модифікуються. Різноманіття та вплив внутрішніх та зовнішніх чинників, які не піддаються кількісній оцінці, призводять до того, що ця не проста система може набувати нові якості, зовсім не властиві її складових компонентів.

Адвокатська діяльність є своєрідним інститутом, що об’єднує складну організаційну структуру, яка містить як з керівні органи, так і органи нижчого так званого рівня. Вони включають Національну асоціацію адвокатів України, Раду адвокатів України, адвокатські ради регіонів, об’єднання адвокатів та окремі адвокати, що практикують індивідуально.

Робота представлена саме ланці адвокатське об’єднання, з його структурою, апаратом, засобами тощо.

Характерною особливістю таких систем є насамперед наявність людини в складових підсистем та її віддаленість від об'єкта її діяльності[1, с. 1]. Це відбувається через те, що немала кількість компонентів, що складають об'єкт інформатизації, інтегрально можуть представляти сукупність трьох груп систем:

1) люди (біосоціальні системи);

2) техніка (приміщення та технічні системи, в яких вони розташовані);

3) програмне забезпечення, яке завжди буває інтелектуальним посередником поміж людиною і технікою (інтелектуальні системи).

Дані групи та їх сукупність утворюють соціотехнічну систему. Уявлення про дану систему зараз є досить поширеним і може стосуватись більшості об’єктів інформатизації. Подальший напрям інтересів обмежується дослідженням систем безпеки, призначених для оброблення вхідної інформації та видачу результату.

Адвокатське об’єднання має власну інфраструктуру, поєднану напряму з людським фактором, і залежить від діяльності людини.

З історії цієї проблеми можна виділити безпосередньо три періоди розвитку засобів захисту інформації (ЗІ):

– перший ми відносимо часу, коли оброблення інформації відбувалося за традиційними (ручними, паперовими) технологіями;

– другий – коли для оброблення даних на регулярній основі використовувалися засоби обчислювальної техніки перших поколінь;

– третій – коли застосування засобів електронно-обчислювальної техніки набрало масового характеру (поява персональних комп'ютерів).

Фактично з появою ПК починається етап затребуваності методів та способів захисту даних, що відносяться до адвокатської таємниці.

У XX ст. період 60–70 рр. проблема захисту даних вирішували за допомогою організаційних заходів. До них належать: заходи по режиму, охорона, сигналізація і програмні найпростіші засоби захисту інформації.

У цей час почали набувати застосовування електронні системи контролю управління доступом, почали з’являтися перші парольні системи розмежування доступу.

Інформація розподілялася по місцях зберігання і обробки актуальною стала проблема з її захистом. Через деякий час з’явились дешеві персональні комп'ютери. Це дало можливість використання мереж ЕОМ (глобальних, локальних, національних і транснаціональних), котрі використовують різні канали зв'язку. Дані чинники сприяють розробці високоефективних систем розвідки і одержання даних. Вони знайшли застосування і на сучасних підприємствах.

Сучасне підприємство є складна система, в рамках якої відбувається захист інформації.

Виділяються такі особливості сучасного підприємства:

– не проста організаційна структура;

– багатоаспектність функціонування;

– дуже висока технічна оснащеність;

– широкі зв'язки з кооперації;

– необхідність широкого доступу до інформації;

– зростання питомої ваги цифрової технології обробки інформації;

– висока питома вага автоматизованих процедур процесів оброблення даних;

- відповідальність і важливість рішень, прийнятих в автоматичному режимі, за допомогою автоматизованої обробки інформації;

- висока концентрація інформаційних ресурсів в автоматизованих системах;

- розподілення компонентів автоматизованих систем на великих територіях;

- накопичення величезних обсягів інформації на технічних носіях;

- інтеграція в єдиних базах даних інформації різної належності і різного призначення;

- довгострокове зберігання на машинних носіях великих обсягів інформації [1, с.2];

- доступ до ресурсів автоматизованих систем з великою кількістю абонентів різних категорій і установ;

- циркуляція інформації в автоматизованих системах між компонентами, також віддалених один від одного.[1, с.2].

Адвокатську діяльність не обійшов стороною цей процес, оскільки значна робота полягає в обробленні великого масиву даних, які імплементуються з інформаційним захистом клієнта.

Отже, створення індустрії перероблення інформації, з однієї сторони, створює об’єктивні передумови підвищити продуктивність праці та життєдіяльності людини, з другої сторони, породжує складні і великомасштабні проблеми. Нагальною з них є забезпечення достовірності і цілісності інформації, яка оброблюється і циркулює на підприємстві (адвокатському об’єднанні).

В 1991 році після проголошення Україною незалежності активна робота розпочалося над системами захисту інформації. Було сформовано нормативно-правову базу, котра регламентувала порядок створення органів та системи із захисту інформації з обмеженим доступом. Таким чином

відбулося прийняття низки нормативно-правових актів, для регулювання суспільно-інформаційних відносин у нашій державі. Також відбулося прийняття Законів України: «Про інформацію», «Про державну таємницю», «Про державну статистику», «Про науково-технічну інформацію», «Про захист інформації в автоматизованих системах», «Про Національну програму інформатизації», «Про основи національної безпеки України».

Закон України «Про інформацію» визначає основне поняття інформації, цей Закон закріпив також право громадян України на інформацію, правові основи інформаційної діяльності, розкрив правові форми міжнародного співробітництва в інформаційній галузі.

Основні принципи інформаційних відносин зазначено у 5 статі цього закону до яких відносять:

- гарантування права на інформацію;
- доступність, відкритість інформації та свобода її обміну;
- об’єктивна складова інформації;
- повнота інформації;
- законність отримання, поширення, використання та зберігання інформації.

Вперше стаття 6 цього закону визначила інформаційну політику держави як сукупність основних способів і напрямів діяльності держави з одержання, поширення, використання та зберігання інформації.[2]

Головні вектори державної інформаційної політики:

- доступ громадян до інформації;
- зміцнення матеріально-технічних, організаційних, фінансових, наукових і правових основ інформаційної діяльності;
- ефективного забезпечення використання інформації;
- сприяння постійному збагаченню, оновленню та зберіганню національних інформаційних ресурсів;
- створення національних мереж і систем інформації;
- створення системи охорони інформації;

- сприяння міжнародному співробітництву в сфері інформації та гарантування суверенітету України щодо інформації.

Інформаційну політику у відповідності до вказаного нормативно-правового акту здійснюють і розробляють органи державної влади загальної компетенції, та спеціальної компетенції[2].

Також в цьому законі вказано право на громадян на інформацію. Відповідно до нормативно-правового акту усі громадяни, юридичні особи та державні органи володіють правами на інформацію, що передбачає можливість вільного отримання, використання, зберігання та поширення відомостей, необхідних для реалізації прав, свобод і інтересів, здійснення функцій і завдань.

Слід зазначити, що закріплення права громадян на інформацію є значним кроком не тільки в правовій розбудові системи інформаційного захисту, а у демократичних завоюваннях поосттоталітарного режиму.

Кожному громадянину надається доступ до інформації, яка стосується його особисто, за виключенням випадків, передбачених законами України [2].

Наступний крок нормативно-правового закріплення органів та системи захисту інформації з обмеженим доступом є прийняття Закону України «Про державну таємницю», що регулює суспільні відносини, пов’язані з тим, що інформація відноситься до державної таємниці, розсекречуванням, засекречуванням її матеріальних носіїв та охороною таємниці маючи на меті захист національної безпеки України.

В законі зазначені органи, що забезпечують охорону інформації з обмеженим доступом – державної таємниці. Цей органом є Служба безпеки України.

Один з нормативно-правових актів, що сформулював правову основу органів захисту інформації та системи з обмеженим доступом, став Закон України «Про державну статистику», котрий регулює правові відносини в сфері державної статистики, визначає функції та права органів державної

статистики, організаційні засади державну статистичну діяльність маючи на меті отримання об’єктивної та всебічної статистичної інформації щодо соціальної, економічної, демографічної та екологічної ситуації в Україні регіонах і забезпечення нею суспільства та держави.

В державних статистичних органах циркулює багато інформації, яка може вплинути безперечно на національну безпеку України, то нормативно-правовий акт сприяє процесу формування системи та органів на яких покладено функції захисту інформації з обмеженим доступом.

У зв’язку з розвитком інформаційно-телекомунікаційних систем і підвищенням циркуляції інформації в автоматизованих системах виникла необхідність належного юридичного оформлення – використання та поширення її через ці засоби[4]. Тому мета Закону України «Про ЗІ в автоматизованих системах» встановлення основ регулювання правових відносин що стосується захисту інформації в автоматизованих системах при умовах дотримання права власності громадян нашої держави та юридичних осіб на інформацію та право доступу до неї, також права власника інформації для її захисту, і встановленого законодавством обмеження на правовий доступ до інформації.

Важливими новелами законодавства, що стали проблемою перед законодавцем, стало забезпечення захисту адвокатської таємниці. В результаті чого прийнято Закон України «Про адвокатуру та адвокатську діяльність», котрий визначає поняття адвокатської таємниці, але питань її захисту в АС не вирішує.

1.2 Методологія розробки КСЗІ в сучасних інформаційно-телекомунікаційних системах з урахуванням специфіки адвокатської діяльності

Інформація, яку, фактично, можна вважати продуктом діяльності, може бути власністю як держави, так і окремих підприємств, установ та людей. Як

і будь-який об’єкт власності, інформацію потрібно захищати. Але проблема захисту інформації є доволі неоднозначною, адже її не можна трактувати лише як захист прав її власників. Вирішуючи проблему захисту інформації, потрібно розглядати такий важливий аспект, як захист прав громадян, які, згідно Конституції, повинні мати вільний доступ до певних відомостей. Теоретичні засади захисту інформації формуються органами державної влади, з врахуванням безпеки держави в цілому.

Згідно з ст. 20, 21 Закону України “Про інформацію”, інформацію можна поділити на

- відкриту;
- інформацію з обмеженим доступом (ІзОД).

Інформацію з обмеженим доступом, в свою чергу, можна поділити на

- конфіденційну;
- таємну;
- службову.

Конференційною інформацією є інформація про фізичну особу, доступ до інформації обмежено самою ж особою, за винятком суб’єктів владних повноважень. Це означає, що особа має право надавати таку інформацію за своєю згодою і на своїх умовах. Оскільки Україна зараз має курс на диджіталізацію усіх сфер життя людини, то, зрозуміло, що інформаційні ресурси формуються у всіх сферах діяльності людини, в тому числі політичній, військовій, економічній, тому інформаційну безпеку необхідно розглядати як комплексний показник національної безпеки. Це твердження визначає важливу роль захисту інформації в рамках національної безпеки країни, особливо в сьогоднішніх реаліях під щоденною загрозою розгортання повномасштабної війни з Росією [3].

В Законі України “Про захист персональних даних” об’єктами захисту є персональні дані, котрі обробляються в базах персональних даних. Персональні дані за режимом доступу є ІзОД [4]. Згідно ст. 8 Закону України “Про захист інформації в інформаційно-телекомунікаційних системах”

“Інформація, котра є власністю держави, чи інформація з обмеженим доступом, вимоги щодо захисту встановлені законом, має оброблятися в системі з використанням комплексної системи захисту інформації” [5].

Проблемою є питання віднесення адвокатської таємниці до таємної інформації, що стосується вимог її захисту в автоматизованих системах. Дивлячись на назву, на перший погляд вона належить до таємної інформації, тому вимоги щодо її захисту є законодавчо не жорсткими. Вказані проблеми будуть розглянуто в наступних розділах.

Згідно вимог законодавства України, з метою забезпечення конфіденційності, цілісності, доступності та спостережності інформації в автоматизованій системі (АС) створюється комплексна система захисту інформації (КСЗІ).

Дослідження формування КСЗІ, що стосується Адвокатського об’єднання «Захист права», як і в інших організаціях, установах, підприємствах базується на загальних принципах, підходах, на спеціальних та загальних методах дослідження. До них відносяться: законності (будь-які дії з інформацією, також її захист можуть відбуватися відповідно до закону – зберігання, збирання, поширення, захист інформації); плюралізму (неможливо охарактеризувати захист адвокатської таємниці не використовуючи різних наукових точок зору дивлячись на складну структуру концепції «адвокатської таємниці»); взаємозв’язку (застосуванню підлягають як базові питання захисту інформації, безпосередньо також питання захисту адвокатської таємниці, інформації конфіденційної, а також комерційної таємниці).

До підходів, які використовуються зупинимося на комплексному підході, КСЗІ включає в себе систему правових, організаційних, інженерно-технічних засобів для захисту інформації.

В роботі використовується методи аналізу (класифікація інформації, модель загроз, модель порушника), синтезу («поглинання» адвокатською

таємницею комерційної та конфіденційної інформації), індукції, дедукції, тощо.

1.3 Висновок до першого розділу

Аналіз викладених вище положень показує, що Україна намагається реалізовувати політику держави щодо захисту інформації. Приймаються відповідні законодавчі акти, впроваджуються та розробляються методики, інструкції, положення тощо. Але, деякі питання ще не повністю врегульовані, що стосуються проблеми захисту адвокатської таємниці в автоматизованих системах.

В рамках проведення дослідження використовуються загальновідомі принципи, методи та підходи, які застосовано для впровадження системи захисту інформації на базі адвокатського об’єднання.

РОЗДІЛ 2 КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ПОНЯТТЯ ТА СТРУКТУРА

2. 1 Поняття комплексної системи захисту інформації

Комплексна система захисту інформації - це система, всебічно і повно охоплює всі предмети, процеси і фактори, котрі забезпечують безпеку інформації, що захищається. Таким чином, з визначення випливає, що тільки комплексна система гарантує досягнення максимальної ефективності інформаційного захисту, оскільки системність забезпечує необхідні захисні компоненти та встановлює між ними технологічний і логічний, а комплексність, вимагає повноти даних складових, забезпечує її надійність.

В Україні за часи незалежності накопичено немалий досвід по захисту інформації. Після низки атак, в результаті яких постраждали, як малі, так і великі компанії усіх форм власності, зараз керівники почали усвідомлювати важливість проведення на підприємстві ряду організаційних заходів та використання спеціалізованих технічних і програмних засоби. Разом з цим, прийшло розуміння, що дуже часто цих окремих кроків є недостатньо для забезпечення безпеки.

Головний підходом захисту інформації вважають комплексний підхід, який полягає не в застосуванні окремих засобів, а швидше виступає регулятором на всіх етапах циклу систем опрацювання інформації та передбачає одночасне застосування різних механізмів захисту [3]. Для захисту інформації важливо не лише використати всі можливі засоби, методи і заходи, максимально раціональним чином об'єднуються в цілісний механізм. За звичай, коли говорять про захист, то мають на увазі захист інформації від цілестрямованих порушників. Проте потрібно пам'ятати, що порушником можна стати ненавмисно, це можуть бути некомпетентні чи недостатньо підготовлені користувачі та працівники. Також захист

інформації, особливо на об'єктах критичної інфраструктури передбачає перлік дій у випадку позаштатних ситуацій будь-якого технічного характеру.

Виділимо проблеми реалізації систем захисту:

– з одного боку, потрібно гарантувати надійний захист інформаційних ресурсів і аутентифікацію в системі: унеможливлення випадкового чи навмисного одержання інформації авторизованими чи неавторизованими користувачами, в тому числі шляхом розмежування доступу до ресурсів і компонент інформаційної системи користувачів усіх рангів [1, с. 1];

– з іншої сторони, системи захисту не мають створювати помітні незручності користувачеві в під час роботи з ресурсами системи[1, с.1].

Проблема високого рівня захисту інформації являється досить складною, вона вимагає для рішення не тільки належного виконання деякої сукупності фізичних, організаційних і технічних, наукових заходів та застосування спеціальних програмно-апаратних засобів і методів, а розроблення комплексної системи організаційно-технологічних заходів, спеціалізованих методів і засобів.

У сфері ЗІ на основі практичних і теоретичних досліджень сформульовано системно-концептуальний підхід до ЗІ.

Під системно-концептуальним підходом розуміють:

– цільова системність, в рамках якої захищеність інформації розглядається як одна з основних частин якості інформації [1, с. 1];

– просторова системність, яка пропонує вирішувати питання захисту з врахуванням зв'язку усіх компонент та підрозділів підприємства[1, с. 1];

– часова системність, передбачає безперервність робіт із захисту інформації, що повинні виконуватись згідно до раніше встановлених планів[1, с. 1];

– організаційна системність, що передбачає узгодження організації робіт по ЗІ і керування ними.

Концептуальність підходу передбачає розроблення несуперечливої концепції, як сукупності обґрунтованих поглядів, рішень і положень для

оптимального варіанту організації і забезпечення надійності захисту інформації, та цілеспрямованого планування всіх робіт щодо ЗІ [1, с. 1].

2.2 Структура комплексної системи захисту інформації

Комплексна система захисту інформації (КСЗІ) - сукупність організаційних та інженерних заходів, наукових підходів та програмно-апаратних засобів, основне призначення яких - забезпечення захист інформації, що циркулює в автоматизованій системі [6].

Компонентами КСЗІ можна вважати:

- організаційні та інженерні заходи;
- комплекс технічного захисту інформації (КТЗІ) (захист від витоку технічними каналами);
- комплекс засобів захисту (КЗЗ) від несанкціонованого доступу (НСД) до ІзОД.

До організаційних заходів відносять:

– концепцію інформаційної безпеки (її створення);

– розробку посадових інструкцій для працівників та обслуговуючого персоналу;

– розробка плану дій на низку аварійних з точки зору безпеки випадків: порушення конфіденційності інформаційних ресурсів системи шляхом НСД, виходу засобів захисту з ладу, аварійного відключення, технічних поломок, виникнення надзвичайної ситуації;

– створення правил адміністрування компонент для інформаційної системи, обліку, розмноження, зберігання, знищення носіїв, що містять інформацію, ідентифікації користувачів;

– навчання користувачів правилам інформаційної безпеки.

Інженерно-технічні заходи – використання комплексу технічних спеціальних засобів з метою захисту інформації. Вибір інженерно-технічних заходів виконується в залежності від рівня захищеності інформації, котрий

необхідно забезпечити. До таких інженерно-технічних заходів можна віднести:

– встановлення охоронної сигналізації;

– облаштування відеоспостереження;

–наявність пожежної сигналізації;

–автоматичне пожежогасіння;

–забезпечення охорони периметра;

–контроль управління доступом;

–збір та опрацювання інформації.

До складу КСЗІ входять засоби та заходи, що реалізують способи, механізми, методи захисту інформації від[6]:

– витоку інформації технічними каналами, до яких належать побічні електромагнітні випромінювання та наведення (ПЕМВН), оптичні, акустичні та інші канали;

– витоку інформації внаслідок несанкціонованого доступу, який може бути отриманий шляхом підключення до апаратури та каналів зв'язку, маскуванням під зареєстрованого абонента, нав'язування хибної інформації, використання закладних пристроїв чи програм, застосування комп'ютерних вірусів та інші[7];

– спеціального впливу на інформацію, який здійснюється шляхом формування полів і сигналів для порушення цілісності інформації чи руйнування системи захисту [6].

При створені КСЗІ можна виділити 6 основних етапів:

1 Формування переліку вимог до КСЗІ в ІТС.

2 Розроблення політики безпеки інформації в ІТС.

3 Розроблення технічного завдання на створення КСЗІ.

4 Розроблення проекту КСЗІ.

5 Введення КСЗІ в експлуатацію.

6 Оцінка якості робіт та захищеності інформації в ІТС.

6 Супроводження КСЗІ .

Нормативні документи які використовуються під час створення КСЗІ зображено на рисунку 2.1.

Рисунок 2.1 - Етапи побудови КСЗІ

На першому етапі аналізуються нормативно-правові акти (державних, відомчих та таких, які діють в межах організації, установи, підприємства), на підставі них може встановлюватися обмеження доступу деяких видів інформації чи заборона такого обмеження, чи визначатися необхідність забезпечення захисту інформації відповідно до інших критеріїв. Визначення присутності у складі інформації, що підлягає автоматизованій обробці, таких її видів, котрі потребують обмеження доступу до неї чи забезпечення цілісності або доступності згідно вимог нормативно-правових актів[1].

Наступним етапом є обстеженні середовищ для функціонування ІТС. На цьому етапі слід проаналізувати всі складові середовища:

- середовище обчислювальної системт;
- навколишнє фізичне середовище;
- середовище користувачів;
- інформацію, що обробляється і технологію її оброблення.

Порядок проведення обстеження виконується у відповідності з ДСТУ 3396.1-96. Оформлюються результати проведення обстеження середовищ функціонування ІТС у вигляді акту і включаються, при потребі, до відповідних розділів плану захисту інформації в ІТС, що розробляється згідно з НД ТЗІ 1.4- 001-2000 [6].

На даному етапі відбувається формування завдання для створення КСЗІ визначається задачі захисту інформації в ІТС, мета створення КСЗІ, варіант розв’язання задач захисту, головні напрями забезпечення захисту, загальна будова та склад КСЗІ, засобів захисту інформації; здійснюється аналіз ризиків (вивчення моделі загроз і порушника, можливих наслідків під час реалізації потенційних загроз, величини завдання можливих збитків та ін.) і визначається перелік потенційних загроз. Оформлюється звіт про виконання робіт на даному етапі та оформлення заявки на розробку КСЗІ – технічного завдання (ТЗ) на створення КСЗІ[7].

На другому етапі створюється політика безпеки. Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001. Оформлення політики безпеки рекомендується у вигляді окремого документу Плану захисту. Вивчення об’єкта створення КСЗІ, проведення науково-дослідних робіт.

Політика безпеки розробляється для ІТС в цілому або, якщо є особливості функціонування окремих компонентів КСЗІ, для кожної окремо компоненти, для окремої функціональної задачі, також для окремої технології обробки інформації тощо

На цьому етапі розробник КСЗІ детально вивчає об’єкт, де створюється КСЗІ, уточнює моделі загроз, потенційного зловмисника та результати аналізу керування ризиками, котрі виконані на попередніх етапах, також виконує при потребі додаткові науково-дослідні роботи, для пошуку шляхів реалізації завдання на створення КСЗІ, після оформлення затверджує звіти з НДР, що виконувалися.

На третьому етапі відбувається розробка технічного завдання на створення КСЗІ. Технічне завдання на створення КСЗІ в ІТС є документом, що визначає організаційно-технічні засади з врахуванням вимог із захисту в ІТС інформації, яка обробляється. Важливими складовими технічного завданням є порядок створення КСЗІ та порядок проведення випробувань

КСЗІ. В технічному завданні також прописується порядок введення в експлуатацію КСЗІ в складі ІТС.

Технічне завдання на створення КСЗІ повинно бути складене з врахуванням комплексного підходу до побудови КСЗІ, котрий повинен об'єднати в єдину систему усі необхідні заходи і засоби захисту від прогнозованих загроз безпеці інформації на всіх етапах життєвого циклу ІТС [7]. Потрібно розуміти ,що ТЗ розробляється не лише для вперше створюваних КСЗІ для ІТС, але й повинне бути складене під час модернізації існуючих ІТС.

На четвертому етапі розробляється проекту КСЗІ. Проект КСЗІ виконується на підставі та у відповідності до ТЗ на створення ІТС . Проект КСЗІ повинен містити організаційні та інженерно-технічні рішення у відповідності з вимогами ТЗ, що дають можливість забезпечити сумісність і взаємодію різних компонентів КСЗІ, також узгодити набір заходів і способів захисту інформації між собою [8].

При розробці проєкту КСЗІ виділяють 3 основних проєкти стадії розробки:

- Ескізний
- Технічний
- Робочий

На стадії розроблення ескізного проекту розробляють попередні проектні рішення КСЗІ та, при потребі, її окремі складові частини, а також розроблення, оформлення, після чого узгодження та затвердження документації на КСЗІ.

Під час розробки технічного проекту виконується розробка: загальних проектних рішень, які необхідні для реалізації вимог ТЗ на КСЗІ; рішень що стосуються структури КСЗІ (організаційної структури, також структури технічних та програмних засобів), алгоритмів функціонування та умов застосування засобів захисту; рішень які стосуються архітектури КЗЗ та якими механізмами реалізуються, що визначаються функціональним

профілем послуг інформаційної безпеки [8]. Виконуються організаційно-технічні заходи забезпечення послідовності розробки КЗЗ, середовища розробки, випробувань, експлуатаційної документації КЗЗ у відповідності до заданих відповідним рівнем гарантій реалізації послуг безпеки згідно із специфікаціями НД ТЗІ 2.5-004, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010[8].

На стадії розроблення робочого проєкту відбувається розроблення, оформлення та затвердження робочої документації та експлуатаційної документації КСЗІ, у разі необхідності, окремих складових частин. Робоча документація має детальні рішення, що стосуються реалізації технічного проекту КСЗІ забезпечення управління КСЗІ також взаємодії компонентів, та документацію для тестування, проведення пусконалагоджувальних робіт, випробувань КСЗІ[7].

На п’ятому етапі вводиться КСЗІ в дію та оцінюється захищеності інформації в ІТС. Підготовка КСЗІ до експлуатації. Виконуються роботи з підготовки організаційної структури та розроблення розпорядчих документів, регламентуючих діяльність із забезпечення захисту інформації в ІТС.

Проводиться навчання користувачів ІТС (технічного обслуговуючого персоналу, користувачів, які мають повноваження управління засобами КСЗІ та ін.) що їх стосується, основним положенням документів Плану захисту, які потрібні їм для дотримання алгоритмів політики безпеки інформації, експлуатації будь-яких засобів захисту інформації тощо, перевірка їх знань користуватись технологіями захисту інформації, які впроваджуються та реєстрація результатів навчання.[7]

На цьому етапі виконується комплектування КСЗІ. Постачальники надають необхідну продукцію (засоби захисту інформації, обладнання, матеріали, та ін.), співвиконавці робіт проводять закріплені за ними етапи. Проводяться підготовчі роботи до проведення оцінки створеної КСЗІ на відповідність вимогам НД ТЗІ засобів захисту, котрі на момент проектування КСЗІ не були сертифіковані [7].

Будівельно-монтажні роботи виконуються при переобладнанні існуючих або при будівництві нових спеціалізованих споруд (приміщень), котрі призначені для розміщення технічних засобів ІТС і працівників, сховищ матеріальних носіїв інформації. Будівельно-монтажні роботи при проведенні враховують вимоги технічного завдання на створення КСЗІ в ІТС[7].

Будівельні роботи виконуються силами організації-власника ІТС чи субпідрядними організаціями з будівельно-монтажним профілем відповідно до проектної документації на будівництво, розробленої проектною організацією згідно з вимогами діючих нормативних документів ДБН А.2.2-2, ДБН 2.2-3-2004[8].

Після завершення будівельних робіт необхідно створити комісію з прийняття робіт, яка включає представника організації-замовника будівництва, проектної та будівельно-монтажної організацій. По результатам роботи комісії складають акт приймання робіт за довільною формою з оцінкою їх відповідності вимогам ТЗІ, що затверджується керівником організації-замовника будівництва[9].

Метою пусконалагоджувальних робіт є:

- монтаж обладнання а також атестація комплексу технічного захисту від витоку технічними каналами;

-встановлення та налагодження КЗЗ;

-перевірка на працездатність засобів захисту інформації при їх комплексній взаємодії та в автономному режимі.

Монтаж ОТЗ ІТС, кабелів, мереж живлення та заземлення виконується відповідно з конструкторською документацією робочого проекту[9].

Результат виконаних робіт оформляється відповідним актом, в якому зазначаються: категорії приміщень, місце розташування обладнання ІТС, межі контрольованих зон приміщень, перелік ОТЗ, ДТЗ і комунікацій, що є в цих приміщеннях. Необхідно також провести оцінку відповідності монтажних робіт вимогам нормативних документів. Можуть бути пропозиції застосування додаткових заходів, впровадження яких є необхідним, коли

неможливо під час виконання монтажних робіт в силу певних об'єктивних причин виконати певні вимоги із розміщення ОТЗ[9]. Відповідальною особою, що затверджує акт є керівник організації, який і вважається власником ІТС [9].

Попередні випробування проводяться відповідно з програмою та методиками випробувань. Дану програму готує розробник КСЗІ, а узгоджує замовник ІТС[7]. Методики та програма випробувань, протоколи розробляються та оформлюються у відповідності до вимог РД 50-34.698. Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ[7].

Метою попередніх випробувань являється перевірка працездатності КСЗІ та визначення можливості для прийняття її у дослідну експлуатацію.

За результатами попередніх випробувань складається “Протоколом випробувань”, де міститься висновок про можливості прийняття КСЗІ у дослідну експлуатацію, перелік виявлених недоліків, заходи необхідні для їх усунення, і терміни, які рекомендуються виконання цих робіт.

По закінченню попередніх випробувань виконується дослідна експлуатація КСЗІ. Під час дослідної експлуатації КСЗІ відбувається:

- тестування технології оброблення інформації, керування засобами захисту, проводиться контроль обігу машинних носіїв інформації, налаштовується авторизація користувачів з розмежуванням доступу до ресурсів ІТС, та відбувається автоматизація контролю за діями користувачів;

- навчання з використання програмно-апаратних засобів захисту інформації та отримання відповідних вмінь та навичок співробітниками СЗІ та користувачами ІТС;

- навчання та перевірка рівня засвоєння знань щодо вимог організаційних та розпорядчих документів на предмет розмежування доступу до технічних засобів та інформаційних ресурсів;

- доопрацювання програмного забезпечення внаслідок виявлених під час тестування помилок;

- додаткове налаштування та конфігурація КЗЗ;
- корекція в разі необхідності експлуатаційної та робочої документації.

Після завершення робіт повинна бути проведена державна експертиза КСЗІ уповноваженими на це органами. Документом, який містить висновок про можливість чи навпаки неможливість представлення КСЗІ на державну експертизу є підписаний акт про закінчення дослідної експлуатації.[8].

Державна експертиза КСЗІ є цілком окремим етапом в рамках випробувань ІТС для подальшого введення в експлуатацію. Проведення експертизи регламентує Положення про державну експертизу. Її метою є визначити наскільки КСЗІ відповідає поставленому ТЗ, вимогам нормативної документації із захисту інформації, а також чи можливо ввести побудовану КСЗІ в складі ІТС в експлуатацію[10].

Якщо державна експертиза виявила певні недоліки, то їх необхідно усунути до завершення експертизи. Порядок усунення недоліків є вхожим до порядку проведення попередніх випробувань. Якщо виявлені недоліки неможливо усунути в ході експертизи, це оформлюється актом, до якого вноситься перелік необхідних рекомендацій та доробок щодо їх виконання. Для перевірки виконання рекомендацій та усунення недоліків проводиться повторна експертиза після завершення робіт [10].

Шостим етапом створення КСЗІ є супроводження КСЗІ. Адже недостатньо розробити КСЗІ, потрібно забезпечити її нормальну роботу і функціонування. На цьому етапі виконуються організаційні роботи щодо керування засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ. Цей етап також покликаний забезпечити гарантійні і післягарантійні технічне обслуговування компонентів КСЗІ [8].

Необхідно зауважити, що структура КСЗІ адвокатського об’єднання може бути однотипною як для органів державної влади, де циркулює службова інформація. В свою чергу, це висвітлює проблему віднесення адвокатської таємниці саме до таємної інформації. Впливає на вирішення

питання про необхідність впровадження технічного захисту інформації від витоку технічними каналами зв’язку чи спеціального впливу на засоби обробки інформації.

2.3 Висновок до другого розділу

Комплексна система захисту інформації (КСЗІ) - сукупність організаційних та інженерних заходів, програмно-апаратних засобів, котрі забезпечують захист інформації в АС. Організаційно-правовими заходами можна реалізувати комплекс відповідний нормативно-правовій базі держави обмежувальних і адміністративних заходів, направлених на оперативне вирішення завдань захисту аналізуючи загрози, регламентації діяльності персоналу і напевно визначення порядку функціонування засобів необхідних для забезпечення інформаційної діяльності та засобів ТЗІ, а також шляхом створення служб, які їх реалізовують. Інженерно-технічні заходи – сукупність спеціальних технічних засобів з метою використання їх для захисту.

Важливим аспектом є те, що вимоги створення КСЗІ є однаковими, незалежно чи в АС циркулює інформація, що є власністю держави, або так звана «приватна інформація», до якої відносяться персональні дані та адвокатська таємниця.

З чого випливає наступне, що нормативними документами не вимагається провадження системи технічного захисту інформації, а доцільність її створення лягає на вибір адвокатського об’єднання чи окремого адвоката.

Зважаючи на дорогу вартісну процедуру для впровадження системи технічного захисту інформації, можливо вона не віднайде застосування на практиці.

РОЗДІЛ 3 ПОБУДОВА КСЗІ АДВОКАТСЬКОГО ОБ'ЄДАННЯ «ЗАХИСТ ПРАВА» З УРАХУВАННЯМ МІЖНАРОДНИХ СТАНДАРТІВ

3.1 Формування вимог до КСЗІ адвокатського об'єднання «Захист права»

3.1.1 Дослідження середовища функціонування

Метою дослідження адвокатського об'єднання «Захист права» є:

- підготовка початкових даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС;
- виявлення базових елементів системи, які безпосередньо чи опосередковано можуть впливати на безпеку інформації;
- аналіз взаємного впливу елементів різних середовищ;
- документування результатів обстеження для їх подальшого використання на наступних етапах робіт.

Проведення обстеження середовищ функціонування автоматизованої системи класу «1» Адвокатського об'єднання «Захист права» здійснювалось відповідно до вимог нормативного документу НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Склад і характеристика цієї комп'ютерної системи наведено нижче:

Присутні 3 об'єкти АС класу 1, які не залежать один від одного:

3 ноутбуки

- Dell Latitude E5440 Intel core i5-4300U/8GB/HDD 1TB
- Lenovo B80 Intel core i3 2330m/8GB/HDD 500GB
- HP x360 Intel core i5 6200U/8GB/HDD 1TB

Операційна система і програмне забезпечення у всіх одне, а саме:

- ОС Windows 10;

- Пакет прикладних програм Microsoft Office 2007;
- Google Chrome;
- Adobe Photoshop CS6;
- Total Commander 7.0;
- Skype;
- Viber;
- Антивірус ESET NOD32;
- Антивірус USB Disk Security;
- ABBYY FineReader – Professional.

З персоналу є три особи персоналу а саме 3 адвоката

Присутній один принтер

3 флешки у кожного з персоналу

Необхідно було, також, дослідити інформацію, опрацювання якої планується здійснювати за допомогою АС. Відповідно до відомостей, що наведені в Акті визначення вищого ступеню доступу до інформації, інформація, яка циркулюватиме в АС класу «1» в Адвокатському об'єднанні «Захист права», матиме вищий ступінь «конфіденційно».

В результаті проведеного аналізу, виявилось, що за режимом доступу інформація, яка планується для опрацювання за допомогою ІТС, поділяється на:

- відкриту інформацію загального користування;
- інформацію з обмеженим доступом – конфіденційна інформація, адвокатська таємниця (далі – ІзОД).

ІзОД зберігається та обробляється в ІТС у вигляді електронних документів створених за допомогою пакету прикладних програм Microsoft Office 2007, Adobe Photoshop CS6 або у роздрукованому паперовому вигляді.

Доступ до ІзОД мають зареєстровані в системі користувачі, що належать до адміністративної ланки об'єднання.

Технологією опрацювання інформації за допомогою ІТС можна вважати наступну: ІзОД буде опрацьовуватися за допомогою ІТС, в якій

створена КСЗІ, тільки зареєстрованими в ІТС користувачами за допомогою прикладних програм Microsoft Office 2007, Adobe Photoshop CS6.

ІзОД, яка буде опрацьовуватися в ІТС, буде зберігатися:

- на жорсткому магнітному диску;

- на пристроях зовнішньої пам’яті: DVD-дисках, CD-дисках, флеш накопичувачах.

Документи, в яких розміщена ІзОД, можуть бути надрукованими за допомогою принтерів, які входять до складу ІТС. Скопіювати інформацію на гнучкі носії та флеш накопичувачі можна лише з дозволу адміністраторів безпеки ІТС.

Характеристики фізичного середовища

До характеристик фізичного середовища відносять: наявність приміщень відповідно до категорій, територіальне розміщення компонентів АС, їх фізичні характеристики, вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки й т.п.

Фізичне середовище Адвокатського об’єднання «Захист права» складається із одного приміщення, яке, в свою чергу, складається з 1 кімнати (рис. 3.1)

- 5 розеток під пристрої;
- 1 принтер;
- 3 ноутбуки;
- 1 вікно;
- 1 датчик пожарної сигналізації;
- 1 датчиків розбитого скла;
- 1 вихід.

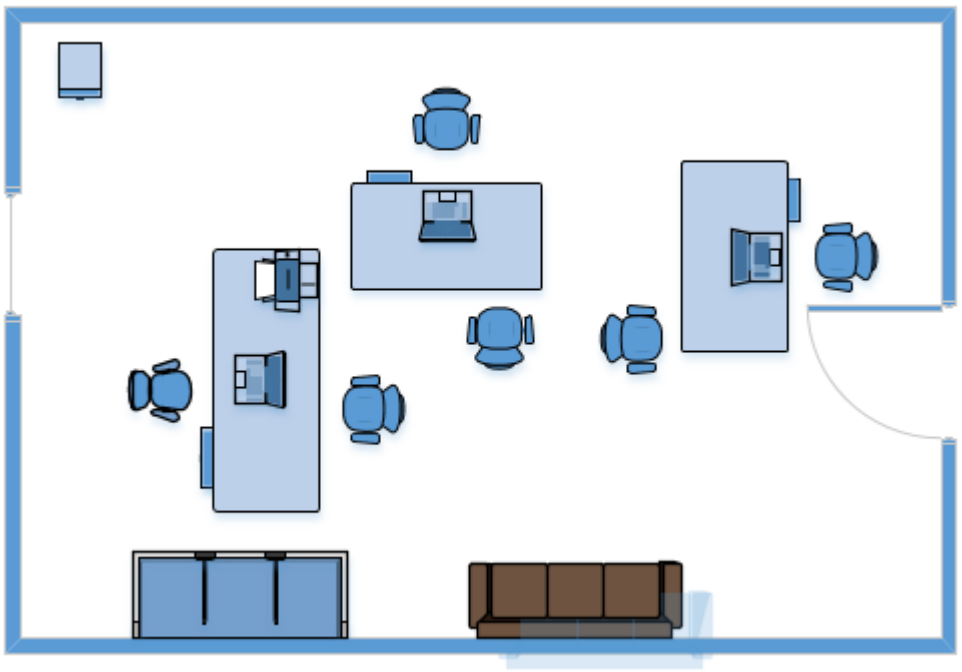

Рисунок 3.1 - План адвокатської організації “Захист права”

Розглянемо контрольовану зону адвокатського об'єднання

3.1.2 Контрольована зона

Контрольована зона - територія, на якій неможливе несанкціоноване перебування сторонніх осіб.

Контрольовану зону визначаєм з будинку, в якому знаходиться АС. Вона знаходиться за адресою м.Тернопіль вул. За Рудкою 33.На вході в будинок стоїть охоронець і на всіх входах є відеокамери. Також на входах на кожний поверх встановлена панель доступу з набору цифр, що унеможливлює НСД на кожен поверх. На наступному рисунку зображені межі контрольованої зони:

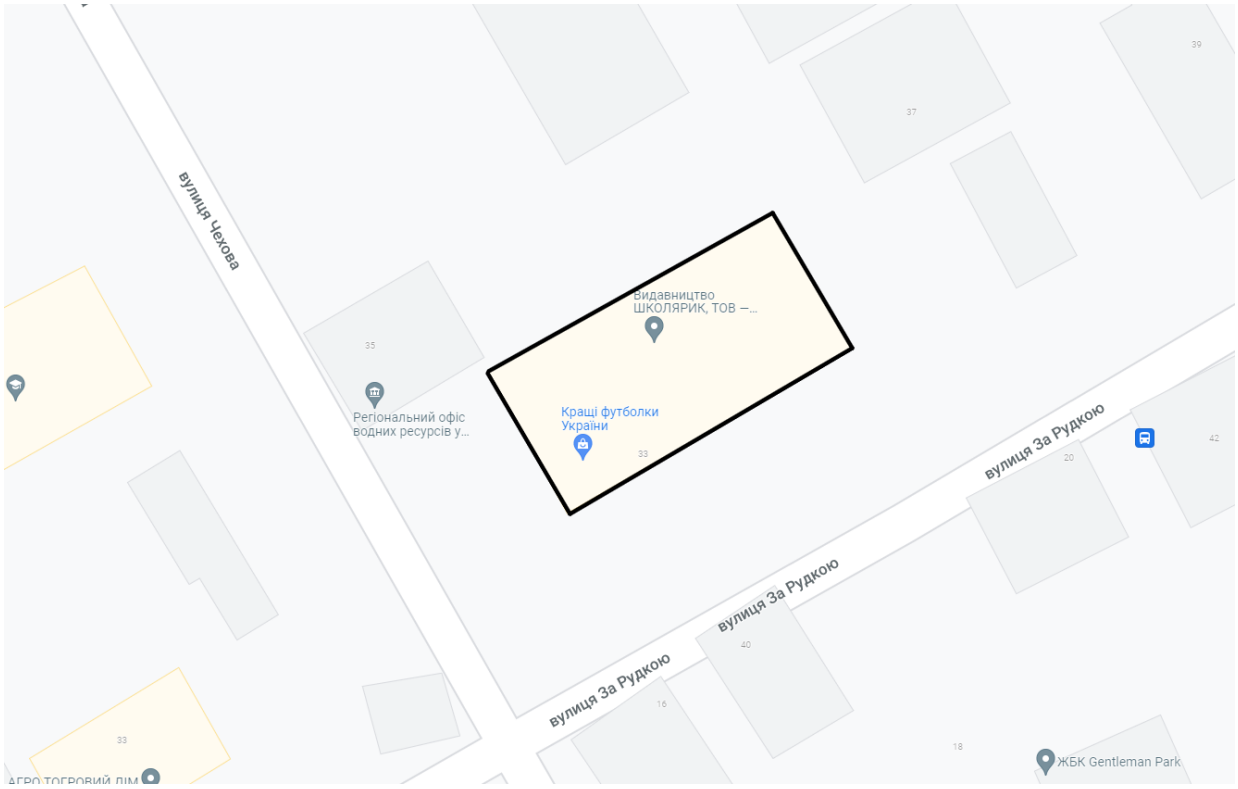

Рисунок 3.2- Межі контрольованої зони

АС знаходиться на 2 поверсі 6 поверхової будівлі.

Внутрішні і зовнішні стіни будівлі зроблені з одинарної цегли(250x120x65 мм) Фундамент – стрічковий, дах виготовлений із профнастилу, уся територія навколо будівлі покрита бруківкою

Так як цегла має ширина цегли 120 мм по нормам зовнішні несучі стіни повинна бути кратною до товщини стіни . Тому вона складає 400 мм(12*3 + 20мм шва між ними). Внутрішні стіни є меншими і складають 251 мм (довжина однієї цегли + шов між ними 10 мм) . Внутрішні перегородки відповідають внутрішнім стінам . В кімнаті з АС є подвійне металопластикове вікно . Двері дерев’яні які закриваються на ключ. Стеля висотою 2,5 метра . Підлога виготовлена з ламінату.

Поверх на якому розташована АС також знаходиться центр поліграфії “Студія друку”

Отже описана вище контрольована зона відповідає усім нормам

3.1.3 Категоріювання інформації

Категоріювання інформації ми вважаємо одним головних етапів створення комплексної системи захисту інформації. Оскільки, в залежності від інформації, яка буде циркулювати в АС, вирішується питання щодо доцільності її захисту.

Цілком зрозуміло, що будь-які дії щодо захисту інформації потребують значних затрат часу та коштів. Відповідно класифікація інформації дає можливість встановити доцільність створення КСЗІ та передбачити необхідні елементи засобів її захисту, що в свою чергу впливає на вартість таких робіт.

До загальної інформації з обмеженим доступом, яка циркулює в даній АС відносимо: конфіденційна інформації (персональні дані адвокатів, працівників, клієнтів), адвокатська таємниця (будь-яка інформація, що ввірені клієнтом адвокату) комерційна таємниця (комерційна діяльність клієнта – суб’єкта підприємницької діяльності).

Конкретизована інформація, яка циркулюватиме на об’єкті інформаційної діяльності – Адвокатського об’єднання «Захист права» представлена в табличці 3.1 .

Таблиця 3.1 – Перелік відомостей що відносяться до конфіденцційної інформації, адвокатської таємниці, комерційної таємниці

№ п/п	Інформація	Обмеження доступу
1.	Відомості про ідентифікатори та паролі адміністратора та інших осіб, що мають доступ до управління АС	конфіденційно
2.	Відомості, що розкривають систему охорони, перепускного режиму, технічного оснащення щодо охорони даного підприємства.	конфіденційно
3.	Відомості стосовно діяльності Адвокатського об'єднання «Захист права»	конфіденційно
4.	Відомості про працівників Адвокатського об'єднання «Захист права»	конфіденційно
5.	Відомості про постачальників Адвокатського об'єднання «Захист права»	конфіденційно

Продовження таблиці 3.1

6.	Відомості про організацію та технічні засоби реалізації АС	конфіденційно
7.	Нормативна та експлуатаційна документація щодо технічних рішень, прийнятих у спеціальних проектах та проектах захисту підприємства	конфіденційно
8.	Технічні заходи щодо захисту конфіденційної інформації, адвокатської таємниці	конфіденційно
9.	Відомості, що розкривають зміст угод, договорів, контрактів, які за домовленістю сторін вважаються конфіденційними	Конфіденційно, комерційна таємниця, адвокатська таємниця
10.	Доповідні записки, довідки, інформаційні листи, методичні рекомендації з питань збереження конфіденційної інформації	конфіденційно
11.	Облікова картка користувача АС про надання доступу до конфіденційної інформації в АС (по заповненню)	конфіденційно

3.2 Розробка політики безпеки для КСЗІ АС класу 1

Під політикою безпеки інформації розуміють, в першу чергу, не один

документ, а сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, в яких втзначено порядок опрацювання інформації, сформовано перелік типових загроз та набір правил для захисту інформації від цих загроз [11].

Основними задачами політики безпеки є можливість:

- гарантувати штатне функціонування АС;
- мати доступ до інформаційних об'єктів та ресурсів АС у відповідності до правил розмежування доступу;
- проводити моніторинг дій користувачів усіх категорій, які мають доступ до АС;
- забезпечувати захист даних у кожному компоненті АС;
- гарантувати достатність та ненадмірність захисту інформації у відповідності з вимогами законодавства;
- забезпечити користувачів усіх категорій відповідними організаційно-розпорядчими документами, які стосуються захисту інформації;
- розробити плани підтримки безперебійної роботи АС та планами її відновлення.

Інформація, опрацювання якої відбувається в АС повинна володіти властивостями конфіденційності, цілісності та доступності. А це означає, що з нею повинно бути неможливо несанкцоновано ознайомитись, скопіювати, розповсюдити без відповідного дозволу, модифікувати, відновити знищену інформацію і т.д.

Адміністративний принцип розмежування доступу полягає в реалізації принципу мінімуму повноважень. Цей принцип повинен бути покладений в основу політики безпеки АС. Згідно з цим принципом право доступу може бути може отримати користувач, в якого є службова необхідність користування цією інформацією, яка прописується в посадовій інтсрукції користувачів в розділі їх посадових обов'язків. [11].

Щоб забезпечити необхідний режим доступу до інформації повинен бути створений відповідальний підрозділ – служба захисту інформації, який

має повноваження щодо організації та впровадження прийнятої політики безпеки в АС[11].

Всі працівники, адвокати Адвокатського об’єднання «Захист права», які беруть участь в обробці інформації в АС, повинні бути зареєстровані як користувачі в системних журналах АС.

Управління правами доступу користувачів до захищених об’єктів та параметрами КЗЗ у складі АС покладається на спеціально визначену особу працівника – адміністратора безпеки АС.

Надання доступу до інформації АС повинно здійснюватися лише на підставі ідентифікації користувачів АС, шляхом розпізнавання їх параметрів. Ідентифікація, автентифікація та авторизація користувачів здійснюється як організаційними заходами, так і з використанням програмно-апаратних засобів розмежування доступу [11].

У випадку встановлення спроби порушення встановленого порядку доступу до інформації, її повинно бути заблоковано.

3.2.1 Нормативно-правові заходи захисту інформації

Комплекс нормативно-правових заходів захисту інформації АС включає в себе наступні етапи:

- імплементація нормативно-правових заходів з забезпечення безпеки інформації в АС,

- забезпечення виконання правових та договірних вимог з захисту інформації;

- визначення відповідальності посадових осіб;

- розробка організаційної структури АС;

- розподіл обов'язків співробітників служби захисту інформації в АС;

- навчання і підвищення кваліфікації персоналу і користувачів АС шляхом ознайомлення з основними тезами політики безпеки інформаціїпроведення тренігів та семінарів, а також впровадження заходів

контролю знань;

- контроль за вчасною, ефективною та повною реалізацією заходів з захисту інформації в АС, дотриманням персоналом і користувачами положень політики безпеки.

3.2.2 Організаційні заходи захисту інформації

Комплекс організаційних заходів захисту інформації в АС включає в себе:

- впровадження режимних заходів на об’єктах інформаційної діяльності;

- побудова фізичного захисту обладнання АС, носіїв інформації, інших ресурсів;

- організація проведення аналізу середовищ функціонування АС;

- проведення робіт з захисту інформації

- взаємодія з іншими суб’єктами системи технічного захисту інформації в Україні;

- регламентація доступу користувачів і персоналу до ресурсів АС;

- здійснення профілактичних заходів, щоб попередити ненавмисне порушення політики безпеки, зокрема передбачити можливу появу вірусів та ін.

Організаційні заходи щодо керування доступом повинні визначати:

- порядок доступу користувачів у приміщення, що захищається, до технічних засобів, носіїв інформації, програмного та інформаційного забезпечення;

- порядок внесення/вилучення даних щодо логінів та паролів доступу користувачів до АС адвокатського об'єднання.

Організаційні заходи щодо реєстрації та обліку повинні передбачати визначення порядку:

- обліку, використання і зберігання машинних носіїв інформації;

- організацію зберігання, використання і знищення документів і носіїв, що містять інформацію з обмеженим доступом, відповідно до вимог нормативних документів.

Організаційні заходи щодо забезпечення цілісності інформації повинні врегулювавувати:

- резервне копіювання інформації, налаштувань операційних систем і функціональних програм;
- порядок обліку, використання і зберігання носіїв інформації, що містять резервні копії операційних систем і функціональних програм;
- забезпечення цілісності системного програмного забезпечення;
- забезпечення цілісності КЗЗ АС адвокатського об'єднання.

3.2.3 Інженерно-технічні засоби захисту інформації

Комплекс інженерно-технічних засобів захисту інформації – сукупність програмно-апаратних засобів захисту для того, щоб:

- розмежувати права доступу користувачів до інформації, баз даних, та інших даних АС;
- заблокувати максимальну кількість несанкціонованих дій з інформацією та іншими ресурсами АС, вміти локалізовувати ці дії по відношенню до ресурсів та ліквідовувати їх наслідки;
- контролювати та захищати потоки інформації, яка обробляється в АС;
- спостерігати в режимі реального часу за діями користувачів та персоналу АС,
- проводити реєстрацію, збір, зберігання, опрацювання даних про івенти, які мають відношення до безпеки інформації, налаштувати систему повідомлень адміністратора безпеки про такі події;
- забезпечувати цілісність ресурсів системи захисту, середовища виконання прикладних програм та інформації, які вважаються критичними;
- контролювати та забезпечувати цілісність об'єктів, що підлягають захисту;
- організовувати облік, зберігання та кругообіг матеріальних носіїв інформації;
- управляти засобами КСЗІ та контролювати основні моменти її функціонування .

Організаційні заходи антивірусного захисту інформації в АС Адвокатського об’єднання «Захист права» повинні передбачати:

- встановлення ліцензійного антивірусного програмного забезпечення на всіх персональних комп'ютерах, що входять до складу АС ;
- моніторинг постійного та вчасного оновлення антивірусних баз.

Автоматизована система даної організації має на меті управління інформацією із метою захисту персональних даних, адвокатської та

комерційної таємниці, що, зокрема, полягає в забезпеченні її цілісності й конфіденційності. Не менш важливу роль відграє забезпечення доступності [12]. Таким чином АС класу 1 відповідає стандартний функціональний профіль захищеності в КС із підвищеними вимогами до забезпечення конфіденційності, цілісності й доступності оброблюваної інформації:

1.КЦД.1 = { КА-1, КО-1,
ЦА-1, ЦО-1,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }

1.КЦД.2 = { КА-1, КО-1,
ЦА-1, ЦО-1,
ДР-2, ДС-1, ДЗ-1, ДВ-2,
НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }

1.КЦД.3 = { КА-1, КО-1,
ЦА-1, ЦО-1,
ДР-2, ДС-2, ДЗ-2, ДВ-2,
НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }

1.КЦД.4 = { КА-1, КО-1,
ЦА-1, ЦО-1,
ДР-2, ДС-3, ДЗ-3, ДВ-3,
НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }

Для того, щоб мати можливість відновити забезпечення інформацію у випадку збоїв системи або помилок користувачів в АС, необхідно проводити час від часу (з певним втановленим інтервалом) резервне копіювання даних.

Резервному копіюванню підлягає:

- ІзОД, яка зберігається у файлах користувачів;
- ІзОД, яка зберігається у БД;
- налаштування ОС;

- журнали реєстрації.

Порядок та періодичність резервного копіювання визначається у спеціалізованій експлуатаційній та організаційно-розпорядчій документації. В ній також повинен визначатись порядок архівування та відновлення інформації, місце збереження резервних копій та відповідальні посадові особи за цей фронт робіт.

КЗЗ повинен проводити розмежування доступу на основі даних користувачів і захищених об'єктів та затверджених правил для кожної категорії користувачів. Розмежування доступу означає надання або встановлення заборони неавторизованому користувачеві прав читати або модифікувати об'єкт.

Адміністратор системи та адміністратор безпеки (відповідно до своїх повноважень) за допомогою КЗЗ повинні визначити перелік конкретних користувачів, які мають право на ознайомлення чи модифікацію для кожного захищеного об'єкта.

Комплекс засобів захисту повинен дозволяти проводити розмежування доступу до сильнозв’язаних об’єктів на підставі імені користувача та його визначеної ролі.

Розмежування доступу до слабозв’язаних об’єктів КЗЗ повинен здійснювати на підставі імені користувача (групи користувачів) і захищеного об'єкта та прав доступу.

Адміністратор БД повинен налаштувати розмежовування доступу до ресурсів серверу управління базами даних за допомогою надання користувачеві певних прав в системі.

Запити на зміну прав доступу (надання прав доступу, внесення користувача до певної групи або надання певної ролі) повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від кола строго визначених осіб.

Персонал має право працювати з текстовими документами, за які вони відповідають, а також працювати із файлами з документами, що

створюються спільно з іншими користувачами, відповідно до наданих прав.

Персонал має право на читання, запис та зміну інформації, що міститься у БД в залежності від програмного комплекса та наданих йому в цьому комплексі прав, а також прикладної ролі, яку він виконує у цьому комплексі.

Обслуговуючий персонал може переглядати та запускати системне та спеціальне програмне забезпечення відповідно до його функціональних обов'язків.

Обслуговуючий персонал не повинен виконувати і не відповідає за налаштування конфігурації КЗЗ, системне та програмне забезпечення, СКБД. Також він не має права встановлювати та налаштовувати ПЗ, змінювати права доступу, тобто виконувати функції будь-кого з адміністраторів.

Щодо реєстрації дій користувачів КЗЗ повинен забезпечити реалізацію наступних функцій:

1) моніторинг та аналіз подій, що мають відношення до безпеки:

- реєстрація користувача в системі (вхід/вихід, час роботи в системі);
- зміна паролю користувачем ;
- зміна прав та повноважень доступу до файлів та ресурсів;
- створення, доступ та знищення файлів;
- запуск програм, які мають доступ до ІзОД.

Обов'язковими параметрами реєстрації мають бути:

- дата, час, та назва події;
- ідентифікатор суб'єкта, що ініціював подію.

2) можливість перегляду журналу подій, що повинні реєструватися, та бажано проводити їх аналіз на предмет виявлення аномалій поведінки;

3) зберігання та захист журналів реєстрації від несанкціонованої модифікації.

Реєстрація дій користувача, пов'язаних з виводом інформації на друк за допомогою принтера, введення інформації за допомогою сканера та

копіювання інформації на з’ємні машинні носії повинна фіксуватися в паперовому “Журналі обліку роботи користувачів ”.

3.3 Модель порушника для Адвокатського об’єднання «Захист права»

Порушниками на об’єктах інформаційної діяльності можуть вважатись суб'єкти, внаслідок навмисних або ненавмисних дій котрих, і (або) випадкові події, внаслідок настання яких можливі реалізації загроз для інформації[13].

Модель порушника – це абстрактний опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, очислювальні потужності, час та місце дії, можливість доступу до інформації і т.ін. Класифікація порушників по відношенню до АС: внутрішні (з числа співробітників, користувачів системи) або зовнішні (сторонні особи)[13].

Модель порушника повинна враховувати:

- можливу мету порушника та його маркування за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник.;
- гіпотезу про кваліфікацію порушника;
- гіпотезу про характер його дій.

Порушник може мати на меті:

- отримати необхідну інформацію у потрібному обсязі та вигляді;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми цілями;
- нанесення збитків шляхом знищення матеріальних та інформаційних ресурсів.

Порушники класифікуються за рівнем можливостей, що надаються їм всіма доступними засобами. (Таблиця 3.2).

Таблиця 3.2 - Класифікація порушників

	Можливості порушника по технологічному процесу	Потенційна група порушників	Можливий результат НСД
1	Ні	Працівникиі, які не мають доступу до інформації, але мають доступ в приміщення (обслуговуючій персонал, відвідувачі)	Перегляд на екрані монітора і розкрадання паперових і машинних носіїв.
2	Запуск задач (програм) з фіксованого набору, що реалізують заздалегідь передбачені функції з обробки інформації.	Більшість користувачів АС, які мають безпосередній доступ до приміщень, з повноваженнями, обмеженими на рівні системи захисту інформації (СЗІ).	Доступ користувача до інформації іншого користувача в його відсутність, в т.ч. через мережу, перегляд інформації на моніторі (недотримання організаційних вимог). Перегляд і розкрадання паперових носіїв.
3	Управління функціонуванням АС, тобто вплив на базове програмне забезпечення ОС і СУБД, на склад і конфігурацію обладнання АС. Робота із зовнішніми носіями.	Адміністратори АС (адвокати), наділені необмеженими повноваженнями стосовно управління ресурсами.	Доступ адміністратора АС до інформації інших користувачів і до засобів СЗІ, ненавмисне руйнування інформації (недотримання організаційних вимог)
4	Весь обсяг можливостей осіб, які здійснюють ремонт технічних засобів АС.	Обслуговуючий персонал АС. Фахівці сторонніх організацій, які здійснюють постачання і монтаж обладнання для АС.	Доступ обслуговуючого персоналу АС до ПК з інформацією інших користувачів, руйнування інформації, установка закладних пристроїв (недотримання організаційних вимог при ремонті АС).

3.4 Модель загроз для інформація яка буде циркулювати в АС 1

Побудова моделі загроз є невід'ємним етапом при розробці КСЗІ. Для цього потрібно скласти перелік загроз та сформуваати їх неформалізований опис. Серед усіх можливих загроз обирають ті, що вважаються найбільш ймовірним для адвокатського об’єднання. Для цього експерти повинні здійснити оцінку імовірності реалізації загрози та умовних втрат внаслідок її реалізації за чотирирівневою шкалою (низький, середній, високий, дуже високий), необхідно також визначити сукупний рівень загрози.

Нижче мною побудована модель загроз, на основі консультацій з експертами та учасниками об'єднання та відповідно до нормативного документу НД ТЗІ 1.4-001-2000. В цій моделі означені властивості захищеності інформаційних об’єктів, які можуть бути порушеними – конфіденційність , цілісність, доступність.

Нормативним документом України «НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі» регламентовано структуру опису загрози, яка враховує властивість, яка порушена та спосіб реалізації загрози.

Властивості інформації або ІТС, які порушує загроза:

- конфіденційність;
- цілісність;
- доступність;
- спостережливість;
- керованість ІТС.

Можливі способи здійснення загрози:

- технічні канали, що включають зокрема канали побічних електромагнітних випромінювань, радіо, хімічні, акустичні, оптичні та інші канали;
- канали спеціального впливу;

- несанкціонований доступ шляхом перехоплення інформації по каналах зв'язку, маскування під зареєстрованого користувача, нав’язування хибної інформації, застосування закладних пристроїв чи програм та нав'язування комп’ютерних вірусів.

Перші два способи за принципом належать до фізичного доступу, останній – це логічний доступ.

Таблиця 3.3- Модель загроз

Потенційні загрози інформації	Властивості, які порушуються			Способи реалізації загрози		
	К	Ц	Д	*	**	***
Фізичне руйнування системи		+	+		+	+
Вимкнення чи виведення з ладу підсистем забечення функціонування.		+	+		+	
Дії з реорганізації функціонування системи			+		+	+
Вторгнення агентів в оточення персоналу системи	+	+	+		+	+
Вербування персоналу чи окремих користувачів, що мають визначені повноваження	+	+	+			+
Перехоплення даних, переданих по каналу зв’язку	+			+		
Перехоплення акустичного випромінювання	+			+		
Розкрадання і вивчення виробничих відходів	+					+
Несанкціоноване перехоплення інформації	+			+		+
Несанкціоноване підключення до технічних засобів	+	+	+			+
Розкрадання носіїв інформації	+	+	+			+
Незаконне заволодіння паролями	+	+				+
Несанкціоноване використання терміналів користувачів	+	+				+
Впровадження програмно-апаратних закладок і вірусів	+	+	+			+

К – конфіденційність;

Ц – цілісність;

Д - доступність;

*— технічні канали;

** — канали спеціального впливу;

*** — шляхом несанкціонованого доступу через підключення до засобів та ліній зв`язку ,маскування під зареєстрованого користувача, нав`язування хибної інформації, застосування програмного-апаратних закладок і впровадження комп`ютерних вірусів.

Об’єктивні дані про імовірність реалізації більшості з наведених загроз насправді отримати дуже важко, а часто і неможливо. Тоому таку імовірність прийнято визначати з допомогою експертів, а для окремих загроз, що є типовими для АС 1-го класу (згідно з НД ТЗІ 2.5-005-99), – емпіричним шляхом, на підставі об'єктивного досвіду експлуатації подібних систем.

Ми взяли до уваги такі шляхи порушення конфіденційності інформації:

К.1.1. Несанкціонований доступ неавторизованих осіб до персональної інформації, що зберігається та обробляється на АРМ ОВР або АРМ ЛОМ ЦВ, через фізичний доступ до обладнання.

Імовірність реалізації – середня.

Оцінка втрат від атаки – високі.

Сукупний рівень ефективності – високий.

К.1.2. Несанкціонований доступ неавторизованих осіб до персональної інформації під час її передачі по відкритих каналах зв’язку та опрацювання на транзитних комутаційних вузлах внаслідок навмисного підключення до каналів зв’язку чи обладнання, помилок під час налаштування комутаційного обладнання або апаратних збоїв.

Імовірність реалізації – низька.

Оцінка втрат від атаки – високі.

Сукупний рівень ефективності – середній.

К.1.3. Несанкціонований доступ неавторизованих осіб до персональної інформації, що опрацьовується в межах центрального або регіонального

вузла доступу, через навмисне підключення до каналів зв’язку чи обладнання з наступним використанням відомих вразливостей програмно-технічних засобів ІТС.

Імовірність реалізації – низька.

Оцінка втрат від атаки – високі.

Сукупний рівень ефективності – середній.

К.1.4. Несанкціонований доступ неавторизованих осіб до персональної інформації, що обробляється в межах центрального або регіонального вузла доступу, через навмисне підключення до каналів зв’язку чи обладнання з наступним використанням перехоплених атрибутів доступу авторизованих користувачів.

Імовірність реалізації – низька.

Оцінка втрат від атаки – високі.

Сукупний рівень ефективності – середній.

К.1.5. Несанкціонований доступ неавторизованих осіб до персональної інформації, що зберігається та обробляється в ІТС, через фізичний доступ до носіїв інформації.

К.2.1 Несанкціонований доступ неавторизованих осіб до технологічної інформації через компроментацію атрибутів доступу авторизованими користувачами (порушення конфіденційності персональної інформації К.1.1, К.1.4).

Імовірність реалізації – середня.

Оцінка втрат від атаки – середні.

Сукупний рівень ефективності – середній.

К.2.2. Несанкціонований доступ неавторизованих осіб до технологічної інформації з боку авторизованих користувачів системи через необережне поводження авторизованих користувачів з атрибутами доступу (порушення цілісності технологічної та персональної інформації Ц.1.3, Ц.2.1, Ц.2.2).

Імовірність реалізації – висока.

Оцінка втрат від атаки – середні.

Сукупний рівень ефективності – високий.

К.2.3. Несанкціонований доступ неавторизованих осіб до технологічної інформації (даних доступу адміністраторів або інших користувачів системи) з боку авторизованих користувачів системи, які використали відомі вразливості програмно-технічних засобів ІТС, які пропустили розробники КСЗІ (порушення цілісності технологічної та персональної інформації Ц.1.3, Ц.2.1, Ц.2.2).

Імовірність реалізації – висока.

Оцінка втрат від атаки – середні.

Сукупний рівень ефективності – високий.

К.2.4. Несанкціонований доступ неавторизованих осіб до технологічної інформації, що зберігається та обробляється в ІТС через фізичний доступ до носіїв інформації.

Імовірність реалізації – середня.

Оцінка втрат від атаки – низькі.

Сукупний рівень ефективності – середній

Ц.1.1. Порушення цілісності персональної інформації, що зберігається на сервері в центральній базі даних, внаслідок технічного збою.

Імовірність реалізації – середня.

Оцінка втрат від атаки – дуже високі.

Сукупний рівень ефективності – високий.

Ц.1.2. Порушення цілісності персональної інформації, що зберігається на сервері в центральній базі даних, неавторизованими особами внаслідок отримання фізичного доступу до обладнання.

Імовірність реалізації – низька.

Оцінка втрат від атаки – високі.

Сукупний рівень ефективності – середній.

Ц.1.3. Порушення цілісності персональної інформації, що зберігається на сервері в центральній базі даних, внаслідок навмисних дій авторизованого користувача в межах його повноважень через помилки в політиці безпеки.

Імовірність реалізації – середня.

Оцінка втрат від атаки – дуже високий.

Сукупний рівень ефективності – високий.

Ц.1.4. Порушення цілісності персональної інформації, що зберігається на сервері в центральній базі даних, внаслідок ненавмисних (помилкових) дій авторизованого користувача будь-якого рівня.

Імовірність реалізації – середня.

Оцінка втрат від атаки – середні.

Сукупний рівень ефективності – середній.

Ц.1.5. Порушення цілісності персональної інформації, що зберігається на сервері в центральній базі даних, внаслідок ураження комп'ютерним вірусом.

Імовірність реалізації – низька.

Оцінка втрат від атаки – середні.

Сукупний рівень ефективності – середній.

Ц.1.6. Порушення цілісності персональної інформації під час її передачі по каналах зв'язку внаслідок навмисних дій неавторизованих осіб (спроби підміни та нав'язування хибної інформації) або інших причин (збоїв телекомунікаційного обладнання тощо).

Імовірність реалізації – низька.

Оцінка втрат від атаки – високі.

Сукупний рівень ефективності – середній.

Ц.2.1. Порушення цілісності технологічної інформації (журнали реєстрації подій) неавторизованими або авторизованими користувачами на основі застосування відомих вразливостей програмно-технічних засобів ІТС або перехоплених креденшіалів доступу уповноваженого персоналу з адміністративними правами.

Імовірність реалізації – низька.

Оцінка втрат від атаки – високі.

Сукупний рівень ефективності – середній.

Ц.2.2. Порушення цілісності технологічної інформації (конфігураційні файли та екзешні файли програмного забезпечення) неавторизовавними або авторизованими користувачами на основі відомих вразливостей програмно-технічних засобів ІТС або перехоплених креденшіалів доступу уповноваженого персоналу з адміністративними правами. Ця загроза створює передумови для подальшого несанкціонованого доступу до інших компонентів ІТС в рамках реалізації загроз К.1.1 – К.1.4, Ц.3.1 або Ц.1.3.

Імовірність реалізації – низька.

Оцінка втрат від атаки – середні.

Сукупний рівень ефективності – середній.

Ц.2.3. Порушення цілісності технологічної інформації, наприклад зміна конфігураційних файлів та екзешників файлів ПЗ, внаслідок попадання в систему комп’ютерного вірусу.

Імовірність реалізації – низька.

Оцінка втрат від атаки – середні.

Сукупний рівень ефективності – середній.

Д.1.1. Втрата доступності персональної інформації, що зберігається на сервері в центральній базі даних, внаслідок поломки комутаційного, серверного обладнання або підсистем живлення (найбільш імовірним вважається вихід із ладу системи електроживлення).

Імовірність реалізації – висока.

Оцінка втрат від атаки – низькі.

Сукупний рівень ефективності – середній.

Д.1.2. Втрата доступності персональної інформації в результаті ураження системи комп’ютерним вірусом (DOS атака, що призводить до перенавантаження серверів та каналів зв’язку віддалених користувачів інтенсивним трафіком. За звичай, таке велике навантаження може генеруватися бот-мережами або вірусами типу «хробак. В такому випадку неможливо обслуговувати клієнтів та виникають відмови в обслуговуванні).

Імовірність реалізації – середня.

Оцінка втрат від атаки – низькі.

Сукупний рівень ефективності – середній.

Ми розглянули тільки загрози із середнім та високим рівнем ефективності (загрози з низьким сумарним рівнем ефективності не враховуються при розробці комплексних систем захисту інформації). Захист від загроз з високим сумарним рівнем ефективності повинен гарантуватися як мінімум двома різними програмними або програмно-технічними засобами чи сукупністю організаційних та технічних заходів.

У рамках захисту від зазначених загроз комплекс засобів захисту також повинен забезпечити виконання певних вимог із забезпеченням спостережності та контрольованості технологічних процесів в ІТС.

Для забезпечення властивостей інформації стосовно дій користувачів по відношенню до конфіденційної інформації повинні реєструватися такі події:

Н.1.1. Комплекс засобів захисту повинен забезпечувати однозначну ідентифікацію користувача, що послав запит на будь-яку дію, пов’язану зі зміною персональної інформації в базі даних, потрібно забезпечити моніторинг таких транзакцій.

Н.2.2. Комплекс засобів захисту повинен виявляти дії користувачів, що перевищують їх посадові обов’язки та можуть бути розцінені як спроби несанкціонованого доступу до інформації.

Для забезпечення властивостей інформації стосовно дій користувачів та адміністраторів щодо технологічної інформації повинні реєструватися такі події:

Н.2.1. Коли користувач категорій 1-2 отримав (рівнів РР, ОВР) доступ до системи (вхід/вихід).

Н.2.2. Фіксувати невдалі спроби отримання доступу до будь-якого компонента системи внаслідок провалу аутентифікації користувача або адміністратора.

Н.2.3. Реєструвати зміни конфігураційних налаштувань компонентів

системи (серверів та мережного обладнання).

Н.2.4. Фіксувати перевищення встановлених адміністратором граничних значень використання системних ресурсів обладнання (процесорного часу, дискового простору).

Н.2.5. Вивляти та блокувати в режимі реального часу несанкціоновані дії користувачів системи, які можуть призвести до атаки внаслідок реалізації відомих вразливостей програмних засобів системи шляхом виявлення аномальної поведінки або ж пошуку відомих сигнатур атак у мережі.

Н.2.6. Виявляти та блокувати в режимі реального часу несанкціоновані дії користувачів, що перевищили свої службові обов’язки з метою отримання несанкціонованого доступу до інформації (сканування портів, отримання прав адміністратора тощо).

3.5 Висновок до третього розділу

Роблячи підсумок, можна сказати, що для побудови якісної КСЗІ, яка б задовольняла всім законодавчим актам України, необхідно використання тільки сертифікованих засобів захисту інформації. Так само необхідний детальний аналіз об'єкта інформаційної безпеки для виявлення всіх вразливих місць Адвокатського об’єднання «Захист права».

Вважаємо, що розробка моделі загроз, моделі порушника, політики безпеки є типовими як для інших підприємств, установ та організацій.

Окрему увагу слід приділити класифікації інформації, яка підлягатиме захисту. Адвокатською таємницею можна повністю охопити весь спектр захищеної інформації (конфіденційної, окрім персоналу, комерційної таємниці). Проте, для кращого розуміння системи захисту слід все ж виокремлювати їх в окремі групи.

Проблемними залишаються питання доцільності захисту адвокатської таємниці від витоку технічними каналами зв’язку, оскільки законодавчо така

вимога не є закріпленою в нормативно-правових актах чи нормативних документах. Така вимога застосовується виключно для державної таємниці. Однак, розкриття чи втрата такої інформації може мати непоправні втрати для клієнта, що в свою чергу може дискредитувати Конституційний принцип права на захист.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Сучасний розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. Сьогодні, напевно, важко уявити компанію, господарська діяльність в якій здійснювалась би без використання комп'ютерної техніки. Через масовий характер робіт, що виконуються працівниками за допомогою комп'ютера, законодавством України чітко врегульовано норми та вимоги до використання комп'ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп'ютером.

Згідно з нормативними актами про охорону праці (НПАОП 0.00-7.15-18) є такі вимоги безпеки до робочих місць працівників з електронними пристроями:

- Площа, відведена на одне робоче місце має становити не менше 6 кв.м., а об'єм – не менше 20 куб.м.

- Конструкція робочого місця повинна забезпечувати підтримання оптимальної робочої пози, тобто такої, яка дозволяє працівникові виконувати роботу з мінімальним напруженням тіла, і яка дозволяє уникнути перевтоми в ході і після закінчення робочого процесу.

- Для забезпечення безпеки та захисту здоров'я працівників усе випромінювання від екранних пристроїв має бути зведене до гранично допустимого рівня (вплив на людину факторів довкілля - шуму, вібрації, забруднювачів, температури тощо, який не спричиняє соматичних або психічних розладів, а також змін стану здоров'я, працездатності, поведінки, що виходять за межі пристосувальних реакцій) з погляду безпеки та охорони здоров'я працівників.

- Організація робочого місця працівника з екранними пристроями має забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним, антропологічним, психофізіологічним вимогам, а також характеру виконуваних робіт.

- Освітлення робочого місця працівника з екранними пристроями має створювати відповідний контраст між екраном і навколишнім середовищем (з урахуванням виду роботи) та відповідати вимогам ДСанПІН 3.3.2.007-98.

- Мікроклімат приміщень з робочими місцями працівників з екранними пристроями має підтримуватись на постійному рівні та відповідати вимогам Санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 42.

Вимоги щодо розміщення ІТС

Приміщення, в яких планується установка та подальша робота з комп'ютером, повинні відповідати проектній документації будинку, погодженій з уповноваженими державними органами. Крім того, роботодавець повинен враховувати санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення, а також характеристики електромагнітного, ультрафіолетового та інфрачервоного полів. Робочі місця, обладнані персональними комп'ютерами, заборонено облаштовувати у підвальних або цокольних приміщеннях будівель. При обладнанні приміщень забороняється використання полімерних матеріалів, що виділяють шкідливі хімічні речовини.

Природне і штучне освітлення

Згідно документу ДБН В.2.5-28:2018 "Природне і штучне освітлення" приміщення з постійним перебуванням людей повинні мати природне освітлення. Природне освітлення поділяється на бокове, верхнє і комбіноване. Що до штучного освітлення воно поділяється на робоче, аварійне, охоронне і чергове.

Для загального штучного освітлення доцільно використовувати розрядні та світлодіодні джерела світла, які за однакової потужності з тепловими джерелами мають більшу світлову віддачу та більший термін експлуатації

Види інструктажів з охорони праці

Працівники, під час прийняття на роботу та періодично, повинні проходити на підприємстві інструктажі з питань охорони праці, надання першої медичної допомоги потерпілим від нещасних випадків, а також з правил поведінки та дій при виникненні аварійних ситуацій, пожеж і стихійних лих.

За характером і часом проведення інструктажі з питань охорони праці (далі - інструктажі) поділяються на вступний, первинний, повторний, позаплановий та цільовий.)

Вступний інструктаж

Проводиться:

- з усіма працівниками, які приймаються на постійну або тимчасову роботу, незалежно від їх освіти, стажу роботи та посади;

- з працівниками інших організацій, які прибули до організації і беруть безпосередню участь у робочому процесі або виконують інші роботи для підприємства;

Вступний інструктаж проводиться спеціалістом служби охорони праці або іншим фахівцем відповідно до наказу (розпорядження) по організації, який в установленому Типовим положенням порядку пройшов навчання і перевірку знань з питань охорони праці.

Первинний інструктаж.

Первинний інструктаж проводиться до початку роботи безпосередньо на робочому місці з працівником:

- новоприйнятим (постійно чи тимчасово) до організації або до фізичної особи, яка використовує найману працю;

- який переводиться з одного структурного підрозділу організації до іншого;

Повторний інструктаж

Повторний інструктаж на робочому місці індивідуально з окремим працівником або групою працівників, які виконують однотипні роботи, за обсягом і змістом переліку питань первинного інструктажу.

Повторний інструктаж проводиться в терміни, визначені нормативно-правовими актами з охорони праці, які діють у галузі, або роботодавцем (фізичною особою, яка використовує найману працю) з урахуванням конкретних умов праці, але не рідше:

- на роботах з підвищеною небезпекою - 1 раз на 3 місяці;

- для решти робіт - 1 раз на 6 місяців.

Позаплановий інструктаж.

Позаплановий інструктаж проводиться з працівниками на робочому місці або в кабінеті охорони праці:

- при введенні в дію нових або переглянутих нормативно-правових актів з охорони праці, а також при внесенні змін та доповнень до них;

- при порушеннях працівниками вимог нормативно-правових актів з охорони

- праці, що призвели до травм, аварій, пожеж тощо;

- при перерві в роботі виконавця робіт більш ніж на 30 календарних днів для робіт з підвищеною небезпекою, а для решти робіт - понад 60 днів.

Цільовий інструктаж.

Цільовий інструктаж проводиться з працівниками:

- при ліквідації аварії або стихійного лиха;

- при проведенні робіт, на які відповідно до законодавства оформлюються наряд-допуск, наказ або розпорядження.

Цільовий інструктаж проводиться індивідуально з окремим працівником або з групою працівників. Обсяг і зміст цільового інструктажу визначаються залежно від виду робіт, що виконуватимуться.

4.2 Безпека в надзвичайних ситуаціях

План реагування на надзвичайні ситуації (далі – НС) розробляється для організації і здійснення взаємоузгодженого комплексу організаційних і практичних дій щодо проведення аварійно-рятувальних робіт з ліквідації наслідків надзвичайних ситуацій, забезпечення у разі загрози або виникнення НС оперативного реагування органів управління, сил та засобів функціональних і територіальних підсистем єдиної державної системи цивільного захисту, запобігання загибелі людей, зменшення матеріальних втрат, організації першочергового життєзабезпечення постраждалого населення та своєчасного надання йому допомоги.

Так як адвокатська організація “Захист права” налічує менше 50 персоналу потрібно використати інструкцію розробленою ДСНС України відповідно статті 130 Кодексу цивільного захисту України та рекомендовано листом від 21 лютого 2015 року № 03-2684/171

ТИПОВА ІНСТРУКЦІЯ

Що до дій персоналу адвокатської організації “Захист права” при загрозі або виникнені надзвичайних ситуацій

1. Загальні положення

Оцінивши існуючі обстановки з питань цивільного захисту та надзвичайних ситуацій в організацій для даної організації найкращим режимом функціонування буде режим повсякденного функціонування. Режим повсякденної діяльності – за нормальної виробничо-промислової, радіаційної, хімічної, біологічної , сейсмічної, гідрогеологічної і гідрометеорологічної обстановки.

Основні заходи, що реалізуються єдиною державною системою у режимі повсякденної діяльності:

- ведення спостереження і здійснення контролю за станом довкілля, обстановкою на потенційно небезпечних об'єктах і прилеглій до них території;

- вдосконалення процесу підготовки персоналу уповноважених органів з питань надзвичайних ситуацій та цивільного захисту населення, підпорядкованих їм сил;

- організація навчання населення методів і користування засобами захисту, правильних дій у цих ситуаціях;

- створення і поновлення резервів матеріальних та фінансових ресурсів для ліквідації надзвичайних ситуацій;

- здійснення цільових видів страхування;

- оцінка загрози виникнення надзвичайної ситуації та можливих її наслідків;

2. Характеристика можливої обстановки в районі підприємства при виникненні надзвичайної ситуації.

Основними джерелами потенційної небезпеками на даній території є:

- Пожежна небезпека

- Погіршення гідрометеорологічної обстановки

3. Порядок оповіщення адміністрації та персоналу про загрозу виникнення надзвичайних ситуацій

Адміністрація у неробочий час оповіщається по телефону. У залежності від обстановки оповіщається і решта персоналу. У робочий час персонал підприємств оповіщається про надзвичайну ситуацію по телефону.

Пункти 4,5,6 можна усунути для даної організації , так як потенційних НС не було виявлено

7. Вимоги до персоналу щодо додержання протиепідемічних заходів при загрозі розповсюдження особливо небезпечних інфекційних захворювань

Якщо на території підприємства або поблизу його виникла небезпека розповсюдження особливо небезпечних інфекційних захворювань, усі працівники повинні суворо виконувати вимоги санітарно-епідеміологічної служби щодо проведення термінової профілактики та імунізації, ізоляції і лікуванню виявлених хворих, дотримуватися режиму, який запобігає розповсюдженню інфекції, при необхідності працівники, які прибули на

роботу, повинні проходити санітарну обробку або дезінфекцію, а також виконувати інші вимоги та заходи, які перешкоджають розповсюдженню особливо небезпечних інфекційних захворювань.

8. Заходи щодо зберігання матеріальних цінностей у період загрози та виникнення надзвичайних ситуацій.

Усі працівники підприємства повинні вжити необхідні заходи щодо зберігання матеріальних цінностей при загрозі або виникненні надзвичайних ситуацій. У період виконання заходів по захисту від надзвичайних ситуацій або при ліквідації їх наслідків необхідно вживати заходи, які направлені на попередження або зменшення можливих збитків організації від них, на забезпечення охорони майна та обладнання.

9. Особливості дій працівників при деяких надзвичайних ситуаціях.

При виникненні пожежі на підприємстві всі працівники зобов’язані суворо виконувати вимоги Інструкції з пожежної безпеки, евакуацію проводити згідно Плану евакуації.

При загрозі або виникненні катастрофічних стихійних лих працівник підприємства по розпорядженню адміністрації повинен зупинити організацію, виконати необхідні протипожежні заходи, відключити від електромережі електрообладнання, підготуватися до евакуації, або вивезення у безпечні місця найбільш цінних матеріальних засобів.

Якщо з’явилися постраждалі-надається перша медична допомога.

ВИСНОВКИ

Враховуючи проведені дослідження, напрошуються висновки, що захист адвокатської таємниці в інформаційно-телекомунікаційних системах є важливим аспектом розвитку сьогодення з урахуванням того, що розвиток правової держави зумовлює певні вимоги щодо захисту особи, якій надається правова допомога.

Така особа повинна бути забезпечена гарантією, що її юридичні питання будуть рівноцінно захищатися як на паперових, так і на цифрових носіях.

В ході проведеної роботи з урахуванням поставлених завдань ми прийшли до наступних висновків:

1. Питання захисту адвокатської таємниці в АС є не до кінця врегульовано законодавцем. Для вирішення проблеми підлягають застосування загальні принципи та підходи. В роботі використано методи аналізу (класифікація інформації, модель порушника, модель загроз), синтезу («поглинання» адвокатською таємницею комерційної таємниці та конфіденційної інформації), дедукції та індукції.

2. Сформовано загальні вимоги та політику безпеки для адвокатського об’єднання. Вважаємо, що розробка політики безпеки є загально типовою як для органів державної влади.

3. Класифікацію інформації, яка підлягає захисту приділили окрему увагу. Встановлено, що усіх типах адвокатських об’єднань циркулюя як правило комерційна таємниця, конфіденційна інформація та безпосередньо адвокатська таємниця.

Впровадження КСЗІ для адвокатського об’єднання обумовлено тими є способами та засобами як і для службової інформації. Тому необхідним є відображення адвокатської таємниці в підзаконних актах та нормативних документах з захисту інформації для більш чіткого розуміння підготовки

КСЗІ. Адвокатська таємниця як окремий вид таємної інформації включає в себе елементи конфіденційної інформації, комерційної таємниці та окрема безпосередньо адвокатської таємниці в розумінні закону. Відповідно доцільно включити адвокатську таємницю як окремий вид інформації в правила захисту інформації в автоматизованій системі для чіткого розуміння стратегії формування системи захисту. Тобто, невизначеним залишається необхідність впровадження елементів захисту від витоку технічними каналами зв'язку та спеціального впливу на засоби обробки інформації. На нашу думку, все ж для адвокатської таємниці потрібно впровадити більш жорсткі вимоги ніж до конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комплексні системи захисту [Електронний ресурс]. – Режим доступу:https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi

2. Методология создания комплексной системы защиты информации / Онацкий А.В. // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 350–356.3

3. Закон України“Про державнутаємницю”[Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/3855-12[Дата доступу] 12.01.2018р.;

4. Закон України “Про захист персональних даних”[Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2297-17 [Дата доступу] 11.09.2018р.;

5. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” ” [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12[Дата доступу] 09.01.2018р.

6. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

7. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу;

9. ДБН А.2.2-3-97 Проектування. Склад, порядок розробки, узгодження і затвердження проектної документації для будівництва;

10. Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом Держспецзв’язку України від 16.05.07 № 93, зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087;

11. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

12. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

13. Малюк А.А. Введение в защиту информации в автоматизированных системах / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2001.

14. Іт політика університету [Електронний ресурс]. – Режим доступу: https://itsecurity.uiowa.edu/enterprise-active-directory

15. Сканування мережі та перевірка на проникнення [Електронний ресурс]. – Режим доступу: https://itsecurity.uiowa.edu/scan-pen-test

16. Правила користування мережею(ResNet) [Електронний ресурс]. – Режим доступу: https://itsecurity.uiowa.edu/resnet

17. Політика повітряного простору [Електронний ресурс]. – Режим доступу: https://itsecurity.uiowa.edu/airspace

18. Мережа громадянства [Електронний ресурс]. – Режим доступу: https://itsecurity.uiowa.edu/networkcitizenship

19. Наказ Департаменту спеціальнихтелекомунікаційних систем та захистуінформаціїСлужбибезпекиУкраїни "Про Положення про державнуекспертизу в сферітехнічногозахистуінформації" від 29 грудня 1999 р. № 62.

20. Указ Президента України "Про заходи щодозахистуінформаційнихресурсівдержави" від 10 квітня 2000 р. № 582/2000.

21. Указ Президента України "Про заходи щодорозвиткунаціональноїскладовоїглобальноїінформаційноїмережіІнтернет та забезпечення широкого доступу до цієїмережі в Україні" від 31 липня 2000 р. № 928/2000.

22. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в

комп’ютерних системах від несанкціонованого доступу;

23.НД ТЗІ 1.1-004-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

24.НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу;

24. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

25. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ 29.03.06 № 373;

26. Мотузко Ф.Я. Охрана праці. – К.: Вища школа, 1989. – 336с.

27.Самгин Е.Б. Освітлення робочих місць. – К.: МИРЭА, 1989. – 186с.

28. Зінченко В.П. Основі ергономіки. – М.: МГУ, 1979. – 179с

29. Белова Н.А. Безпека життєдіяльності. - М.: Знание, 2000 - 364с

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.056
І. І. Забавчук

(Тернопільський національний технічний університет ім. І. Пулюя)

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ АДВОКАТСЬКОГО ОБ'ЄДНАННЯ "ЗАХИСТ ПРАВА"

UDC 004.056

I. I. Zabavchuk

INFORMATION PROTECTION IN AN AUTOMATED SYSTEM OF THE LAWYERS' ASSOCIATION "ZAKHYST PRAVA"

Автоматизація пронизує усі сфери нашого життя, зокрема не обійшла стороною і адвокатську діяльність.

Автоматизація у загальному сенсі полягає у застосуванні технічних засобів, економіко-математичних методів та систем управління, що звільняють людину частково чи повністю від безпосередньої участі у процесах отримання, перетворення, передачі та використання енергії, матеріалів чи інформації.

Автоматизована система — організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [1].

В автоматизованій системі АО «Захист права» інформаціє є об'єктом захисту, в ній циркулює таємна інформація і персональні дані про клієнтів та адвокатів.

Відповідно до статті 22 Закону України «Про адвокатуру та адвокатську діяльність» адвокатською таємницею є будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених цим Законом підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, зміст порад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності [2].

Незважаючи на той факт, що законодавством адвокатську таємницю віднесено до таємної інформації, все ж вимоги щодо її захисту в автоматизованих системах залишаються на рівні конфіденційної інформації.

Тому при організації автоматизованих систем повинні суворо дотримуватися вимоги захисту конфіденційних даних, які покликані запобігти їх витоку або спотворенню. Захист інформації в автоматизованій системі повинен запобігти впливу загроз різного походження, включаючи техногенні аварії, помилок конфігурацій і програмного забезпечення, вплив шкідливого програмного забезпечення або хакерів, зловживанням службовими повноваженнями, викрадення даних інсайдерами з метою продажу або шпигунства. Зменшити рівень таких ризиків дозволяє реалізація комплексу заходів захисту апаратного та програмного рівня.

Таким чином, приходимо до висновку, що слід ретельно доопрацювати нормативні документи щодо захисту інформації в автоматизованих системах, окремо приділивши

увагу адвокатській таємниці в частині врегулювання питання її місця в структурі інформації з обмеженим доступом.

Література

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Офіційний сайт Верховної ради України [Електронний ресурс]: Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
2. Закон України «Про адвокатуру та адвокатську діяльність». Офіційний сайт Верховної Ради України [Електронний ресурс]: Режим доступу: https://zakon.rada.gov.ua/laws/show/5076-17#Text