ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙІНСТИТУТ МЕНЕДЖМЕНТУ ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему: «Вплив засобів інформаційної безпеки на роботу органів державного управління»

на здобуття освітнього ступеня магістра
зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
освітньо-професійної програми Управління інформаційно-комунікаційною діяльністю

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ольга ВЕРТЕЦЬКА

Виконав: здобувач вищої освіти
групи ДЗДМ-61 Ольга ВЕРТЕЦЬКА
Керівник: Світлана ЯРЕМЕНКО,
к.філол.н., доцент
Рецензент: Вікторія КАЧМАЛА,
к.іст.н., доцент

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут менеджменту та підприємництва

Кафедра документознавства та інформаційної діяльності

Ступінь вищої освіти магістр

Спеціальність 029 Інформаційна,бібліотечна та архівна справа

Освітньо-професійна програма Управління інформаційно-комунікаційною діяльністю

ЗАТВЕРДЖУЮ
Завідувач кафедри документознавства та інформаційної діяльності
_____ Тетяна СИДОРЕНКО
«____»_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Вертецької Ольги Анатоліївни

1. Тема кваліфікаційної роботи: Вплив засобів інформаційної безпеки на роботу органів державного управління.

керівник кваліфікаційної роботи Світлана ЯРЕМЕНКО, к.філол.н., доцент
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи «16» грудня 2024р.

3. Вихідні дані до кваліфікаційної роботи:
Мета дослідження: дослідити засоби інформаційної безпеки та їх вплив на роботу органів державного управління, зокрема на їхню здатність забезпечувати надійний захист інформаційних ресурсів, ефективну взаємодію між підрозділами, оперативність прийняття рішень, а також підвищення рівня довіри громадян і протидію сучасним кіберзагрозам.
Об’єкт дослідження - засоби інформаційної безпеки, які використовуються в органах державного управління.
Предмет дослідження - вплив засобів та інструментів інформаційної безпеки на захист інформації та ефективність роботи органів державного управління на прикладі Державної служби якості освіти України.
Перелік питань, які потрібно розробити
1. Аналіз засобів інформаційної безпеки та їх вплив на органи державного управління
2. Аналіз інформаційної безпеки
3. Визначення перспектив впровадження новітніх засобів інформаційної безпеки

4. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання «09» вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Визначення тематики, вибір наукового керівника, уточнення теми	09.09.2024	виконано
2	Розроблення та складання плану кваліфікаційної магістерської роботи	17.09.2024	виконано
3	Підготовка 1 розділу	08.10.2024	виконано
4	Підготовка 2 розділу	29.10.2024	виконано
5	Підготовка 3 розділу	22.11.2024	виконано
6	Висновки	29.11.2024	виконано
7	Підготовка остаточного варіанта роботи	12.12.2024	виконано
8	Написання відгуку науковим керівником	13.12.2024	виконано
9	Оформлення та представлення роботи на кафедру та перевірка на плагіат	16.12.2024	виконано
10	Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія	18.12.2024	виконано
11	Попередній захист роботи	20.12.2024	виконано
12	Основний захист кваліфікаційної магістерської роботи	21.01.2025	виконано

Здобувачка вищої освіти _____ Ольга ВЕРТЕЦЬКА

Керівник кваліфікаційної _____ Світлана ЯРЕМЕНКО

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 78 стор., 3 дод., 48 джерел.

Метою магістерської роботи є теоретичне обґрунтування поняття «інформаційна безпека», вивчення принципів роботи засобів інформаційної безпеки в органах державного управління, а також виявлення перспектив та особливостей впровадження новітніх засобів.

Об'єкт дослідження – засоби інформаційної безпеки, які використовуються в органах державного управління.

Предмет дослідження – вплив засобів та інструментів інформаційної безпеки на захист інформації та ефективність роботи органів державного управління на прикладі Державної служби якості освіти України.

Короткий зміст роботи: У роботі досліджено сутність поняття «інформаційна безпека» та її засоби. Проаналізовано та обґрунтовано перспективи впровадження новітніх засобів інформаційної безпеки в роботу ДСЯО. Окреслено загальну характеристику діяльності ДСЯО. Розглянуто наукову літературу стосовно засобів інформаційної безпеки, який показав, що принципи сучасного захисту інформації можна сформулювати як пошук оптимального балансу між доступністю та безпекою. З'ясовано перспективи впровадження новітніх засобів інформаційної безпеки в роботу ДСЯО. Визначено вплив діяльності органів державного управління на інформаційну безпеку України.

Ключові слова: інформаційна безпека, органи державного управління, інформаційні технології, засоби інформаційної безпеки.

ABSTRACT

Text part of the qualification work for obtaining a master's degree: 78 pages, 3 appendices, 46 sources.

The purpose of the master's work is to theoretically substantiate the concept of "information security", study the principles of information security tools in state administration bodies, as well as identify the prospects and features of implementing the latest tools.

The object of the study in the work is the State Education Quality Service of Ukraine.

The subject of the study is information security tools used in state administration bodies, and their impact on information protection and work efficiency.

Summary of the work: The work explores the essence of the concept of "information security" and its tools. The prospects for implementing the latest information security tools in the work of the NSDF are analyzed and substantiated. The general characteristics of the NSDF activities are outlined. The scientific literature on information security tools is reviewed, which showed that the principles of modern information protection can be formulated as a search for the optimal balance between accessibility and security. The prospects for introducing the latest information security tools into the work of the NSDF have been clarified. The impact of the activities of state administration bodies on the information security of Ukraine has been determined.

Keywords: information security, state administration bodies, information technologies, information security tools.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – інформаційні технології

ДСЯО – Державна служба якості освіти України

АСКОД – програмне забезпечення для зовнішнього юридично значимого документообігу, який дозволяє виконувати погодження, підписання та обмін електронними документами між суб'єктами правовідносин.

ІБ – інформаційна безпека

ПІ – персональні інформаційні технології

ТЗІ – технічний захист інформації

ДУНБ – державне управління національною безпекою

СБУ – служба безпеки України

ЗМІСТ

ВСТУП

ІБ є невід'ємним елементом загальної проблеми забезпечення інформації особистості, держави і суспільства. Вона зосереджена на захисті важливих або вже згаданих питань джерел інформації, законних інтересів. Зміст поняття «ІБ» розкривається в практичній діяльності, наукових дослідженнях, а також нормативних документах.

Актуальність дослідження. Проблема захисту інформації існувала ще до появи комп'ютерів і не є новою. Проте розвиток комп'ютерних технологій суттєво вплинув на підходи до забезпечення безпеки інформації. Спочатку системи ІБ розроблялися для військових відомств, оскільки розголошення такої інформації могло призвести до серйозних втрат, зокрема людських. Тому в перших системах безпеки особлива увага приділялася конфіденційності, тобто нерозголошенню інформації. Для надійного захисту повідомлень і даних від розголошення та перехоплення використовувалося їх повне шифрування.

Аналіз останніх досліджень і публікацій. Останні дослідження в ІБ показали, що вона є одним з найважливіших понять в науці і в різних сферах людської діяльності. Сутність і складність цього поняття розкривається природою сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття «ІБ» дає можливість відзначити недоцільність жорсткого вибору тієї чи іншої посади. ІБ виступає як характеристика стійкого, стабільного стану системи, яка під впливом внутрішніх і зовнішніх загроз і ризиків зберігає основні характеристики для свого існування.

У своїх працях досліджували такі науковці як Г.Албул[4], І.Бідюк, С.Шевченко[6], Ю.Глущенко[19], С.Гнатюк[20], А.Приймак[20].

Метою кваліфікаційної роботи є дослідити засоби інформаційної безпеки та їх вплив на роботу органів державного управління, зокрема на їхню здатність забезпечувати надійний захист інформаційних ресурсів, ефективну взаємодію між підрозділами, оперативність

прийняття рішень, а також підвищення рівня довіри громадян і протидію сучасним кіберзагрозам. Для досягнення цієї мети передбачається вирішення окреслених **завдань дослідження:**

- вивчити основні поняття, принципи та нормативно-правову базу, що регулює інформаційну безпеку в органах державного управління;
- проаналізувати типи органів державного управління ;
- дослідити класифікацію засобів інформаційної безпеки;
- оцінити, як засоби інформаційної безпеки впливають на функціонування органів державного управління, їхню ефективність і стійкість до кібератак;
- дослідити перспективу впровадження засобів інформаційної безпеки у роботу служб.;
- запропонувати шляхи вдосконалення системи інформаційної безпеки в органах державної влади для підвищення їхньої ефективності та стійкості до сучасних викликів.

Об'єкт дослідження – засоби інформаційної безпеки, які використовуються в органах державного управління.

Предмет дослідження – вплив засобів та інструментів інформаційної безпеки на захист інформації та ефективність роботи органів державного управління на прикладі Державної служби якості освіти України.

Методи дослідження. У кваліфікаційній роботі застосовуються як загальнонаукові, так і спеціальні методи дослідження. Їх використання дозволяє провести всебічний аналіз засобів інформаційної безпеки, їх впливу на функціонування органів державного управління, а також оцінити ефективність впроваджених технологій і підходів.

Джерельна база дослідження включає наукові статті, положення, Закони України, а також офіційні документи та нормативно-правові акти, що регулюють питання інформаційної безпеки в державному секторі.

Положення, які були використані: «Про організацію системи безпеки електронної пошти Державної служби якості освіти України», «Про порядок

надання доступу працівникам Державної служби якості освіти України до використання прикладних програм, баз даних та інформаційних ресурсів».

Наукова новизна полягає в тому, що ми запропонували нові підходи до захисту інформації від сучасних загроз. Зокрема, ми досліджували, як можна поєднати сучасні методи криптографії (шифрування) з системами виявлення кібератак, щоб швидше і ефективніше захищати дані в реальному часі. Також ми звернули увагу на важливість комплексного підходу до захисту, де враховуються всі рівні безпеки, від технічних засобів до управлінських рішень.

Практичне значення одержаних результатів полягає у тому, що результати науково дослідження допоможуть підвищити готовність органів до нових загроз та удосконалити навчальні програми для працівників, сприяючи таким чином стабільності та безпеці державного управління.

Структура роботи. Кваліфікаційна робота включає в себе вступ, в якому відображена актуальність теми дослідження, сформульовано об’єкт, предмет, мету і завдання дослідження, 3 розділи, в яких досліджуються поставлені завдання, висновок, додатки і список використаних джерел та літератури.

РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АНАЛІЗ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Огляд наукової літератури стосовно засобів інформаційної безпеки

Проблема захисту інформації існувала ще до появи комп'ютерів і не є новою. Проте розвиток комп'ютерних технологій суттєво вплинув на підходи до забезпечення безпеки інформації. Спочатку системи ІБ розроблялися для військових відомств, оскільки розголошення такої інформації могло призвести до серйозних втрат, зокрема людських. Тому в перших системах безпеки особлива увага приділялася конфіденційності, тобто нерозголошенню інформації. Для надійного захисту повідомлень і даних від розголошення та перехоплення використовувалося їх повне шифрування.

Сучасна ситуація характеризується тим, що основним завданням стає захист інформації в комп'ютерних мережах, де зростає важливість безпеки даних, оскільки їх передача та зберігання стають все більш вразливими до різноманітних загроз.

Широке впровадження комп'ютерів у всі сфери діяльності, постійне збільшення їх обчислювальних потужностей та використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною майже будь-якої діяльності [3,с.230].

Принцип сучасного захисту інформації можна сформулювати як пошук оптимального балансу між доступністю та безпекою. Це означає, що система повинна забезпечувати своєчасний доступ до необхідної інформації, водночас захищаючи її від несанкціонованого доступу чи змін. Важливо знайти таке співвідношення, яке забезпечить високу рівень безпеки без

надмірного обмеження доступу до ресурсів, що може вплинути на ефективність роботи системи [5,с.90].

В умовах глобалізації та зростання важливості інформації Конституція України проголошує ІБ «справою всього українського народу». Це, безумовно, декларація, оскільки захист ІБ держави не може бути лише народною справою, для цього передбачено існування спеціальних державних органів. Проте недоліки та прогалини в чинній системі ІБ можуть мати негативні наслідки для матеріального та духовного добробуту народу. У 1997 році Верховна Рада України ухвалила «Концепцію національної безпеки України», яка визначає загрози національній безпеці, зокрема, як «інформаційну експансію з боку інших держав, витік інформації, що становить державну таємницю, а також конфіденційної інформації, яка є власністю держави». Інформаційна безпека була визначена як одна з головних цілей «Національної програми інформатизації» (1998 р.). Цим питанням займається комісія з питань ІБ при Президентові України[2,с.300].

ІБ є важливим аспектом, однак її чітке визначення в нормативних актах відсутнє. На сьогодні є кілька неофіційних визначень ІБ, які не завжди узгоджуються між собою. Одне з них можна знайти в проєкті Закону «Про інформаційний суверенітет та інформаційну безпеку України». У цьому проєкті ІБ визначається як «захищеність життєво важливих інтересів суспільства, держави та особи, якою виключається заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації, негативні наслідки функціонування інформаційних технологій або через розповсюдження забороненої інформації, відповідно до законів України».

Дослідники визначають кілька ключових характеристик ІБ, що допомагають краще зрозуміти її важливість у сучасному контексті:

1. Баланс між національною безпекою та інформаційною функцією держави: ІБ є важливим аспектом на стику між захистом національних інтересів і забезпеченням ефективного функціонування інформаційних процесів у державі.

2. Екстериторіальний характер: ІБ не обмежується національними кордонами, оскільки інформаційні загрози можуть виникати ззовні і стосуватися глобальних процесів.

3. Протистояння між державними інтересами і правами громадян: Існує постійне напруження між бажанням держави засекречувати певну інформацію і правом громадян на вільний доступ до неї, що є важливим аспектом демократії

4. Правова основа державного регулювання: Управління інформаційною сферою повинно відбуватися виключно на основі законів і правових норм, забезпечуючи справедливість та прозорість.

Таким чином, об'єктом ІБ є інформація, яка є критично важливою для функціонування держави, демократичного розвитку суспільства, а також інформаційні стосунки між особою, державою та суспільством, з акцентом на захист інформаційних прав людини як невід’ємної частини загальнолюдських прав.

Згідно з законодавством України, інформація, яка є власністю держави та знаходиться в користуванні органів державної влади, місцевого самоврядування, підприємств, установ та організацій усіх форм власності, може мати обмежений доступ із метою збереження конфіденційності. Така інформація може отримати статус конфіденційної і бути захищеною від розголошення.

Однак, існують певні виключення, коли доступ до інформації не може бути обмежений.

Порядок обліку, зберігання та використання цієї інформації визначається Кабінетом Міністрів України, щоб забезпечити ефективний контроль і захист державних та суспільних інтересів[34,с.60].

Європейська конвенція про захист прав людини та основних свобод (1950 р.) є важливим документом для визначення інформаційних прав людини. Ось ключові моменти, які стосуються інформаційної безпеки та прав людини:

Стаття 10:

Право на свободу вираження поглядів: кожна людина має право на свободу вираження своїх поглядів, включаючи свободу одержувати, передавати та отримувати інформацію та ідеї без втручання органів державної влади та незалежно від кордонів.

Обмеження прав:

У той же час ця свобода не є абсолютною і може бути обмежена в інтересах:

Громадської безпеки;

Запобігання злочинам;

Охорони здоров’я і моралі;

Запобігання розголошенню конфіденційної інформації.

Ці винятки можуть бути застосовані лише за умови, що обмеження прав є необхідними в демократичному суспільстві, тобто такі обмеження повинні бути чітко обґрунтовані і відповідати принципам правової держави.

Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру (1981 р.):

Цей документ був розроблений для захисту інформаційних прав людини, зокрема персональних даних, що обробляються автоматизовано, особливо в умовах сучасних комп’ютерних мереж.

Мета Конвенції: Гарантування свободи інформації незалежно від кордонів і забезпечення безперешкодного обміну інформацією між народами.

Зміст Конвенції включає:

Право на захист персональних даних: кожна особа повинна мати контроль над обробкою своїх особистих даних.

Прозорість обробки даних: перед тим як збирати і використовувати персональні дані, організації повинні повідомляти користувачів про мету і спосіб обробки їхніх даних.

Обмеження обробки даних: дані повинні оброблятися тільки за умови згоди особи, і не повинні передаватися без необхідності.

Ці принципи забезпечують захист особистої інформації та право на приватність в епоху цифрових технологій, що є надзвичайно актуальним в сучасному інформаційному суспільстві.

Директива Європарламенту та Ради Європи від 15 грудня 1997 року є ще одним важливим міжнародним документом, який регулює обробку персональних даних і захист права на приватне життя в телекомунікаційному секторі. Основною метою цієї директиви є забезпечення невтручання в особисте життя при обробці персональних даних, що здійснюється в межах телекомунікаційних послуг, а також сприяння вільному переміщенню персональних даних між країнами Європейського Союзу[20,с.140].

Основні аспекти директиви:

1. Захист права на приватність: Директива гарантує, що персональні дані, які обробляються в телекомунікаціях, не повинні порушувати право громадян на невтручання в особисте життя. Це означає, що збір і обробка таких даних мають бути здійснені з повною повагою до приватності осіб.

2. Регулювання обробки персональних даних: Директива вимагає, щоб операції з персональними даними в телекомунікаційному секторі здійснювались прозоро, і щоб суб'єкти даних мали чітке уявлення про те, як їхні дані обробляються. Технічні та організаційні заходи повинні бути введені для захисту даних від несанкціонованого доступу, зміни або знищення.

3. Вільне переміщення даних: Директива підтримує принцип вільного переміщення персональних даних між країнами ЄС, оскільки безбар'єрний обмін даними є важливим для ефективного функціонування внутрішнього ринку ЄС. Проте, це переміщення може бути обмежене у випадках, коли існують ризики для безпеки або конфіденційності даних.

4. Винятки: Як і в інших європейських актах, директива передбачає певні винятки, коли обмеження права на приватність і обробку даних може бути виправдано:

- Громадський порядок: забезпечення законності та порядку, в тому числі боротьба з тероризмом і організованою злочинністю.

- Оборона та державна безпека: інформація може бути оброблена без згоди осіб у випадках, що стосуються національної безпеки, економічного добробуту держави чи інших питань, що мають стратегічне значення.

- Кримінальне право: забезпечення правосуддя, зокрема у випадках, коли дані необхідні для розслідування чи здійснення судового процесу.

Ця директива має великий вплив на захист персональних даних та приватність в сучасному цифровому середовищі, особливо з огляду на зростаюче використання телекомунікаційних технологій для обміну інформацією[18,с.108].

Державні стандарти та нормативні документи, що стосуються ТЗІ, регулюють вимоги до захисту інформації від неправомірного доступу, втручання, змін або знищення. В Україні ці стандарти встановлюють правила і норми, які мають дотримуватись організації, що працюють з чутливою інформацією.

Основні документи, що регулюють ТЗІ:

1. ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення": Цей стандарт визначає основи ТЗІ, що є важливою для національної безпеки, бізнесу та громадян. Він встановлює об'єкти, мету і принципи організаційно-технічного захисту, а також типи загроз, які можуть виникати при неправомірному доступі до даних.

2. ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт": У цьому документі визначено порядок виконання робіт з ТЗІ. Це включає процедури впровадження засобів захисту, моніторинг систем безпеки, а також методи оцінки ефективності захисту даних.

3. ДСТУ 3396.2-96 "Захист інформації. Технічний захист інформації. Терміни та визначення": Стандарт містить перелік термінів, що використовуються у сфері ТЗІ, а також їхні точні визначення. Це важливо для

забезпечення єдності розуміння термінів серед фахівців і для правильного застосування інших нормативних документів.

Ці стандарти регулюють діяльність всіх організацій та установ, що працюють з інформацією, яку необхідно захищати технічними засобами. Вимоги цих стандартів обов'язкові для:

- підприємств і установ всіх форм власності та підпорядкування;
- громадян-суб'єктів підприємницької діяльності;
- органів державної влади та місцевого самоврядування;
- військових частин і інших військових формувань;
- представництв України за кордоном.

Вони створюють основу для побудови систем ТЗІ, що повинні гарантувати конфіденційність, цілісність і доступність даних.

1.2 Сутність поняття «інформаційна безпека» та її засоби

Характерною рисою сучасного етапу економічного і науково-технічного прогресу є бурхливий розвиток ІТ, їх максимально широке використання як у повсякденному житті, так і в державному управлінні.

Інформація та ІТ все більше визначають розвиток суспільства і служать новими джерелами національної сили. Становлення інформаційного суспільства докорінно змінює політичну, екологічну та соціальну сфери людського життя. У цих умовах формування інформаційного суспільства відбувається зміна предмета роботи в галузі інформації та знань. У свою чергу, основою глобалізації є інтеграція інформаційних систем різних держав в єдину глобальну інформаційну систему, формування єдиного інформаційного простору, створення глобальних інформаційних і телекомунікаційних мереж, інтенсивне впровадження нових ІТ у всі сфери суспільного життя, в тому числі і в державне управління[14,с.45].

Процес глобального інформаційного суспільства охопив практично всі країни світу і в даний час знаходиться в основі науково-технічного і соціально-економічного розвитку.

ІТ - це організаційний, соціально-економічний і науково-технічний процес створення оптимальних умов для комплексного задоволення інформаційних потреб і реалізації прав громадян, суспільства, органів державної влади та адміністрації на основі формування і використання інформаційних ресурсів, мереж, ресурсів та ІТ з використанням комп'ютерного та комунікаційного обладнання.

Основними завданнями інформатизації є:

1. всебічне інформаційне забезпечення потреб суб'єктів інформаційних відносин;
2. створення єдиного безпечного інформаційного простору;
3. створення, впровадження і використання інформаційних систем, ІТ і інформаційних продуктів загального значення;
4. підготовка кадрів, підвищення їх кваліфікації у сфері інформатизації.

Розуміння сутності змісту поняття «ІБ» є важливим завданням наукового аналізу. Будь-яке вчення досягає зрілості і досконалості тільки тоді, коли воно розкриває сутність досліджуваних явищ, має здатність передбачати майбутні зміни не тільки в сфері явищ, але і в сфері субстанцій. Пізнання сутності ІБ можливо тільки на основі абстрактного мислення, створення теорії досліджуваного предмета, усвідомлення внутрішнього змісту, виявлення характерних рис, розкриття ключових ознак досліджуваного поняття.

В історичному процесі формується структура суб'єкта, тобто єдність внутрішнього змісту і зовнішніх проявів, що збігаються і не збігаються щодо суперечливих сутностей. Суть полягає в сукупності глибинних зв'язків, взаємозв'язків і внутрішніх закономірностей, що визначають основні риси і

тенденції розвитку системи. Одна і та ж сутність може мати безліч різних явищ[44,с.113].

Сутність проявляється і розуміється у визначенні, що виражає загальне поняття. Це поняття безпеки по відношенню до ІБ, яке характеризує конкретний процес управління загрозами і ризиками. Отже, під специфічним поняттям «ІБ» розуміється процес управління загрозами і ризиками в інформаційній сфері.

Саме тому ІБ є невід'ємною частиною загальної безпеки, чи то національної, чи то регіональної, чи то міжнародної. Аналіз ІБ передбачає розгляд сукупності таких об'єктивних чинників:

1. потреб громадян, суспільства і держави і світового співтовариства;
2. уразливість індивідів, суспільства і держави від цифрових технологій;
3. наявність широкого кола загроз і небезпек, якими має управляти система забезпечення ІБ.

ІБ є невід'ємним елементом загальної проблеми забезпечення інформації особистості, держави і суспільства. Вона зосереджена на захисті важливих або вже згаданих питань джерел інформації, законних інтересів. Зміст поняття «ІБ» розкривається в практичній діяльності, наукових дослідженнях, а також нормативних документах.

Слід зазначити, що в науковій літературі досі відсутній єдиний уніфікований погляд на поняття «ІБ». Для одних вона відображає стан, для інших - процес, діяльність, здатність, систему гарантій, власність, функцію. Тому виникає необхідність групування напрямків визначення аналізованого поняття.

Українські дослідники вважають за необхідне визначати ІБ як стан безпеки. Наприклад, В.К.Гасеський, В.А.Авраменко визначають ІБ як стан захисту життєво важливих інтересів особи, суспільства і держави, що виключає можливість заподіяння їм шкоди внаслідок недосконалості,

несвоєчасності та недостовірності інформації, внаслідок негативних наслідків функціонування ІТ або в результаті поширення забороненої або обмеженої до поширення інформації, а О.Г.Додонов визначає ІБ як стан безпеки космосу інформації, яка забезпечує формування і розвиток цього простору в інтересах особистості, суспільства і держави[1,с.46].

Аналогічної точки зору дотримується і інший російський дослідник А.С.Панарін, роблячи більший акцент на ролі політичної еліти, яка може протистояти впливу інформації. На його думку, ІБ – це стан інформаційного середовища суспільства та політичної еліти, що забезпечує його формування та розвиток в інтересах керівництва, громадян та суспільства країни.

Дещо в іншому ракурсі трактує інформаційну безпеку А.А.Тер-Акопов, який репрезентує позицію другого напряму. Він розглядає ІБ під дещо іншим кутом. Під ІБ він розуміє той стан, який забезпечує життєво важливі інтереси людини. В рамках цього напряму ІБ визначається як стан, тенденції розвитку, умови життєдіяльності суспільства, його структур, інститутів і інститутів, в яких їх якість підтримується об'єктивно визначеними в ньому нововведеннями і вільними, відповідними його природі і функціям. Деякі представники цього напрямку розглядають ІБ як ситуацію, що характеризується відсутністю ризику, тобто факторів і умов, що безпосередньо загрожують з боку інформаційно-комунікаційного середовища особистості, спільноті, державі. Прихильники цього підходу розглядають ІБ як стан і процес захисту особистості, суспільства і держави від реальних або потенційних загроз. У той же час, на нашу думку, не зовсім коректно розглядати безпеку тільки як державу і не відображає динамізму як самої безпеки, так і системи, для якої безпека функціонує як функція її подальшого розвитку та існування.

Під поняттям процесу розуміється послідовність ситуацій, зв'язок стадій зміни і їх розвитку, тобто, на відміну від поняття "стан", поняття "процес" акцентує увагу на моменті орієнтації на зміну об'єкта, постановку

цілей, в той час як "стан" відображає тільки один момент, певний момент безпеки, а тому не вичерпує його повністю.

Представник третього напряму В.І.Ярочкін визначає безпеку як «стан захисту особистості, суспільства і держави від зовнішніх і внутрішніх небезпек і загроз, в основі якого лежить діяльність людей, суспільства, держави, світової спільноти по виявленню (вивченню), запобіганню, ослабленню, усуненню і відсічі небезпек і загроз, здатних їх знищити, залишити фундаментальні матеріальні і духовні цінності, завдати неприйнятної шкоди, перекрити шлях до поступального розвитку». Застосування діяльнісного підходу, на нашу думку, є більш прийнятним для опису інформаційної безпеки, і в якійсь мірі ми можемо підтримувати це визначення в загальних рисах, але ми не згодні з деталями сфер діяльності, які будуть змінюватися з часом і, отже, підвищувати потенціал нестабільності як у самому визначенні, так і в діяльності зацікавлених суб'єктів.

М.П.Хріпков вважає, що діяльність із забезпечення особистості, суспільства і держави виникає в ході вирішення протиріччя між такою об'єктивною реальністю, як небезпека, і потребою розумного суб'єкта, соціального індивіда, соціальної групи в запобіганні її можливих шкідливих наслідків. У той же час, в даному випадку робота системи ІБ обмежується тільки реагуванням, в той час як профілактика не береться до уваги.

Наступний погляд виходить з того, що в найбільш загальному вигляді під ІБ можна розуміти здатність суб'єкта зберігати системоутворюючі властивості, ключові характеристики при патогенних, руйнівних, катастрофічних впливах на кібернетичні, інформаційні та комунікаційні технології.

На думку прихильників цієї точки зору, безпека і захищеність - це різні поняття, в зв'язку з тим, що безпека виражає характеристику становища соціальної спільноти, в той час як забезпечення безпеки - це характеристика діяльності органів державної влади та адміністрації з підтримання безпеки. У

цьому відношенні безпека розуміється як основа вироблення політики, а безпека - як діяльність, спрямована на досягнення безпечного статусу суспільства або соціальної групи[24,с.134].

Цікавою є думка відомого українського дослідника з проблем інформаційної безпеки В.І.Калюжного, який вважає, що ІБ – це вид правовідносин публічної інформації щодо створення, підтримки, захисту та захисту бажаних для людини, суспільства і держави безпечних умов життя. соціально-правові відносини, пов'язані зі створенням, поширенням, зберіганням та використанням інформації.

В цілому ІБ покликана забезпечувати реалізацію національних інтересів за допомогою всього арсеналу інструментів, що є в її розпорядженні. У цьому сенсі вважаю, що найвищим змістом політики інформаційної безпеки є вільний розвиток і процвітання суспільства.

Таким чином, ІБ є одним з найважливіших понять в науці і в різних сферах людської діяльності. Сутність і складність цього поняття розкривається природою сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття «ІБ» дає можливість відзначити недоцільність жорсткого вибору тієї чи іншої посади.

Концепції, що підходять до визначення ІБ, дозволяють більш комплексно і системно розглянути цю проблему, додати знання про це багатогранне явище. Більш того, на наш погляд, найбільш прийнятним є комплексний підхід, при якому вона буде визначатися шляхом опису її найважливіших базових характеристик з урахуванням безперервної динаміки інформаційних систем.

Такий підхід дозволив зробити висновок, що ІБ не може розглядатися лише як окрема держава. Безсумнівно, це також властивість, характеристика інформаційного суспільства, діяльність і результат людської діяльності, спрямованої на забезпечення певного рівня безпеки в сфері інформації. ІБ повинна враховувати майбутнє і тому є не державою, а процесом. Таким чином, вона повинна розглядатися через органічну єдність таких ознак, як

держава, власність, а також управління загрозами і ризиками, в якому забезпечується найкращий спосіб їх усунення та мінімізації впливу негативних наслідків.

Отже, ІБ — багатогранна область діяльності, в якій успіх може принести лише системно-комплексний підхід. Дослідження сутності її має враховувати той факт, що сутність є внутрішнім змістом предмету, який знаходить вираз у стійкій єдності усіх багатоманітних і суперечливих формах буття.

Критерієм ефективності ІБ є високий рівень безпеки при мінімальних супутніх витратах.

Таким чином, можна говорити про структуру поняття ІБ. Основним її елементом є життєві інтереси соціальної системи, які корелюють із зовнішніми факторами у вигляді інтересів наднаціональних або інших національно-державних структур у межах міжнародного співтовариства. Через національно-державне утворення її життєві інтереси взаємодіють з інтересами елементів, що входять до складу цього формування. До останніх належать соціальні групи, еліти, організації, партії, релігійні та етнічні формування, рухи тощо. Сукупність внутрішніх та зовнішніх інформаційних загроз створює умови для порушення безпечного функціонування системи державного управління.

Важливість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення ІБ як одне з глобальних і першочергових завдань національної політики безпеки[39,с.150].

Як вже зазначалося, національні інтереси у сфері інформації випливають із національних цінностей. Таким чином, інтереси ІБ випливають з таких цінностей, як права людини, свобода та економічне процвітання. Саме тому головним інтересом України є її виживання як вільної незалежної нації зі збереженням фундаментальних цінностей та безпекових інститутів.

ІБ виступає як характеристика стійкого, стабільного стану системи, яка під впливом внутрішніх і зовнішніх загроз і ризиків зберігає основні характеристики для свого існування. Відтак вона може описуватися за допомогою терміну "гомеостазис".

До характеристик, за допомогою яких можна описати дану систему, належать:

1. доступність — можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб'єктом виконавчої влади;
2. цілісність — актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;
3. конфіденційність — захист від несанкціонованого ознайомлення.

Сутність і зміст ІБ проявляються по-особливому на кожному з рівнів державного управління, зокрема на:

1. стратегічному — Кабінет Міністрів України;
2. тактичному — центральні органи виконавчої влади;
3. оперативному — місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації.

Таким чином можна говорити і про прояви ІБ у самому процесі її забезпечення, таким чином можна виділити наступні рівні:

1. нормативно-правововий — закони, нормативно-правові акти тощо;
2. адміністративний — дії загального характеру, які вживаються органами державного управління;
3. процедурний — конкретні процедури забезпечення ІБ;
4. програмно-технічний — конкретні технічні заходи забезпечення ІБ

Для того щоб розкрити сутність і зміст ІБ, важливо пов'язати останню з політикою держави.

Невід'ємною частиною політики держави як регулятора суспільних відносин відповідно до гуманітарних принципів є обов'язок забезпечувати інформаційну безпеку особистості, суспільства і держави.

У найзагальнішому вигляді питання безпеки набагато складніші і вирішуються абсолютно по-різному на міжнародному, національному та особистому рівнях безпеки.

ІБ як одна з характеристик сталого розвитку функціонує як основна цінність держави. У той же час ціннісні орієнтації, засновані на ідеях інформаційної безпеки різних соціальних груп і індивідів, частково не збігаються. Тут він знаходить безпосереднє вираження впливу держави, що виражає загальні цінності в області інформаційної безпеки за допомогою системи методів.

ІБ — складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживанням владою та іншими явищами, що загрожують національній безпеці України; неухильне дотримання конституційного права громадян на свободу слова, доступ до інформації, недопущення незаконного втручання органів державної влади, органів місцевого самоврядування, їх працівників у діяльність засобів масової інформації, дискримінації у сфері інформації та переслідування журналістів за політичні посади; здійснення комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України[25,с.50].

Інформаційні відносини — відносини, які виникають у всіх сферах життя і діяльності людини, суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Інформаційний суверенітет – це здатність держави контролювати та регулювати потік інформації за межі держави з метою дотримання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційний простір (національний):

1. інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту та поширення інформації, інформаційних продуктів та джерел інформації, що підлягає віданні держави;

2. сукупність національних інформаційних джерел та інформаційних інфраструктур, які дають змогу на основі єдиних принципів і загальних правил забезпечити взаємодію громадян, суспільства і держави з інформацією на рівних засадах з їх рівним правом доступу до відкритих інформаційних ресурсів і якнайповнішим задоволенням інформаційних потреб суб'єктів держави на всій її території, дотримуючись балансу інтересів для входження в світовий інформаційний простір і забезпечення інформаційна безпека відповідно до Конституції України та міжнародно-правових норм.

Інформаційна інфраструктура - сукупність взаємодіючих систем для виробництва, накопичення, підтримки та розробки інформаційних продуктів та їх доставки, виробництва інформаційних технологій, систем обслуговування інфраструктури та навчання персоналу.

Інформаційна система являє собою організаційно впорядковану сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

Інформаційні ресурси:

1. сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

2. організована сукупність інформаційних продуктів певної мети, які необхідні для задоволення інформаційних потреб громадян, суспільства, держави в певній сфері життя або діяльності.

ІТ:

1. цілеспрямовано організована сукупність інформаційних процесів з використанням ІТ-обладнання, що забезпечує високу швидкість обробки даних, швидкий пошук інформації, її поширення, доступ до джерел інформації незалежно від їх місця розташування;

2. навмисно організований комплекс інформаційних процедур для створення та використання інформаційних продуктів або надання інформаційних послуг;

3. технологічний процес, предметом перероблення й результатом якого е інформація;

4. процес матеріалізації знань у продукцію і послуги за допомогою комп'ютерно-телекомунікаційних систем;

5. система методів і способів використання комп'ютерної техніки та систем зв'язку для створення, пошуку, прийому, відображення, реєстрації, накопичення, підтримки, захисту та розповсюдження інформації.

Інформаційне середовище – це усталене поєднання окремих тем національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, які взаємодіють у розвідувальних процесах.

Інформаційний ринок - це система економічних, організаційних і правових відносин щодо купівлі-продажу інформаційних ресурсів, технологій, товарів і послуг[32,с.26].

Інформаційний продукт (продукція):

1. документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

2. документована інформація, яку підготовлено відповідно до потреб користувачів і яка призначена чи застосовується для задоволення потреб користувачів;

3. створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

Інформаційна підтримка: підтримка за допомогою систем баз даних і баз знань виробничої, торговельної, управлінської, професійної, науково-дослідної та будь-якої іншої діяльності в усіх секторах суспільства, які спрямовані на створення умов для задоволення інформаційних потреб особистості, суспільства і держави.

Інформаційне поле:

1. сукупність енергетичних субстанцій окремих об'єктів, які є елементами інформаційного поля Землі та Всесвіту;

2. просторово-часові вібрації (інформаційно-розпорядницькі структури), що містять відомості про минуле, сьогодення і майбутнє Всесвіту.

Інформаційне суспільство:

1. суспільство, в якому більшість працівників зайнята створенням, збором, відображенням, записом, накопиченням, збереженням і поширенням інформації, особливо її вищої форми – знань;

2. суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються інформаційно-комунікаційними технологіями

Інформатизація:

1. сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, спрямованих на створення умов для задоволення інформаційних потреб громадян і суспільства на основі створення, розвитку та використання інформаційних систем, мереж, ресурсів та ІТ, які базуються на використанні сучасного інформаційно-комунікаційного обладнання;

2. діяльність, спрямована на створення та широкомасштабне використання в усіх сферах життя суспільства ІТ.

Інформатика – наукова діяльність, що вивчає інформаційні структури та процеси збирання (придбання, придбання), візуалізації, запису, накопичення, зберігання та розповсюдження (розповсюдження, продажу) інформації за допомогою комп'ютерів[42,с.136].

Інформація:

1. фактична або публічно викладена інформація про події та явища, що відбуваються в суспільстві, державі та навколишньому середовищі;

2. відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються у всіх сферах державної діяльності, життя суспільства та навколишнього середовища незалежно від форми їх уявлень) будь-які знання про предмети, події, поняття тощо. проблемні зони, якими обмінюються користувачі системи обробки даних.

Інформаційна війна - процес боротьби між суб'єктами із застосуванням інформаційної зброї.

Інформаційна зброя - це засоби, що дозволяють здійснювати продумані дії з повідомленнями, які передаються, обробляються, створюються, знищуються і сприймаються.

Інформаційна загроза - вхідні дані, спочатку призначені для активації алгоритмів в інформаційній системі, що відповідають за нормальний режим роботи.

Сугестія - прихований інформаційний вплив на інформаційну систему, що самонавчається.

Сугестивний вплив - вплив з формування у інформаційної системи, що самонавчається, прихованих від неї самої цілей.

Беручи до уваги той факт, що структура внутрішньої системи ІБ неможлива поза контекстом загроз і ризиків, наступним елементом, який слід розглянути, будуть загрози ІБ, які в сукупності будуть описувати напрямки роботи системи ІБ.

1.3 Класифікація засобів інформаційної безпеки

ІБ є важливим аспектом діяльності державних установ, підприємств, організацій та окремих осіб у сучасному інформаційному суспільстві. Вона забезпечує захист інформаційних ресурсів. До таких загроз належать несанкціонований доступ, крадіжка чи змінювання даних, атаки, збої в роботі інформаційних систем та інші дії, що можуть спричинити шкоду організаціям чи державним інтересам.

Засоби ІБ є комплексом технологічних, організаційних, правових і фізичних засобів, спрямованих на запобігання, виявлення та реагування на загрози в інформаційних системах. Ці засоби використовуються для забезпечення цілісності, конфіденційності та доступності інформації, а також для збереження її від пошкоджень чи втрат[22,с.85].

У цій роботі буде розглянута класифікація засобів ІБ, їхні основні категорії та особливості.

1. Технічні засоби забезпечують захист на рівні апаратного та програмного забезпечення. Вони використовуються для засобів технічної ІБ

та реалізації основних принципів ІБ, таких як конфіденційність, цілісність та доступність. Технічні засоби можна поділити на кілька підкатегорій.

1.1. Антивірусне програмне забезпечення

Антивірусні програми є одними з основних інструментів для захисту комп'ютерних систем від шкідливих програм, таких як віруси, трояни, шпигунські програми та інші загрози. Вони працюють за принципом виявлення, блокування та видалення шкідливих програм, що можуть порушити роботу інформаційних систем.

1.2. Системи виявлення та запобігання вторгненням (IDS/IPS)

Ці системи дозволяють відстежувати мережеву активність і виявляти підозрілі або несанкціоновані спроби доступу до системи. Системи IDS (Intrusion Detection System) виявляють порушення безпеки, тоді як IPS

(Intrusion Prevention System) не лише виявляють, а й запобігають таким атакам.

1.3. Шифрування даних

Шифрування є одним із основних методів забезпечення конфіденційності інформації. Воно передбачає перетворення даних у такий вигляд, що вони стають недоступними для несанкціонованих користувачів. Шифрування застосовується як до збережених даних, так і до даних, що передаються по мережі[7,с.98].

1.4. Системи резервного копіювання

Ці системи забезпечують збереження даних і відновлення їх у разі пошкодження або втрати. Регулярне резервне копіювання є важливою складовою частиною плану безпеки інформаційної системи.

1.5. Контроль доступу

Засоби контролю доступу дозволяють визначити, які користувачі мають доступ до певних ресурсів системи. Вони включають в себе паролі, біометричні дані, смарт-карти, а також технології багатофакторної аутентифікації.

2. Засоби організаційної ІБ

Організаційні засоби стосуються процесів і процедур, які забезпечують реалізацію політик безпеки. Вони спрямовані на встановлення правил і стандартів щодо доступу, обробки та зберігання інформації

2.1. Політики та регламенти безпеки

Політики безпеки визначають основні принципи та правила для користувачів і системних адміністраторів. Вони охоплюють питання управління доступом, захисту даних, реагування на інциденти та інших аспектів інформаційної безпеки.

2.2. Навчання та підвищення кваліфікації персоналу

Навчання співробітників є важливим елементом організаційної безпеки. Працівники повинні бути ознайомлені з політиками безпеки, а

також з основними методами захисту інформаційних ресурсів, зокрема з підозрілими електронними листами, фішингом, соціальною інженерією тощо.

2.3. Управління ризиками

Цей процес передбачає виявлення потенційних загроз для інформаційної безпеки, їх оцінку і розробку заходів для мінімізації цих загроз. Управління ризиками є ключовим елементом для забезпечення належного рівня захисту інформаційних систем.

2.4. Аудит і моніторинг

Регулярний аудит безпеки дозволяє виявляти вразливості в інформаційних системах і перевіряти їх відповідність вимогам безпеки. Моніторинг допомагає оперативно виявляти інциденти безпеки та реагувати на них.

3. Засоби правової ІБ

Правові засоби включають в себе нормативно-правову базу, яка регулює захист інформаційних ресурсів, а також механізми юридичної відповідальності за порушення безпеки.

3.1. Законодавство

Важливою складовою правової ІБ є законодавчі акти, які регулюють питання збереження та захисту інформації. В Україні такими є закони, як «Про основи національної безпеки України», «Про захист персональних даних», «Про інформацію» тощо.

3.2. Угоди та контракти

Захист інформації також забезпечується через укладання угод та контрактів, які визначають обов'язки сторін щодо захисту конфіденційних даних.

3.3. Захист інтелектуальної власності

Правова безпека також включає в себе захист авторських прав та прав на інтелектуальну власність, що дає змогу уникнути несанкціонованого використання інформаційних продуктів.

4. Засоби фізичної ІБ

Фізичні засоби забезпечують захист інформаційних ресурсів від фізичних загроз, таких як крадіжка, стихійні лиха, пожежі.

4.1. Системи контролю доступу

Ці засоби включають в себе використання ключів, карток, біометричних даних для фізичного обмеження доступу до будівель і серверних приміщень.

4.2. Системи відеоспостереження

Вони дозволяють відслідковувати події на території організації і забезпечувати контроль за доступом до критичних ресурсів.

4.3. Пожежна та кліматична безпека

Забезпечення безпеки від стихійних лих, таких як пожежі чи затоплення, здійснюється через використання сучасних систем сигналізації та контроль кліматичних умов.

5. Засоби оперативної та тактичної ІБ

Ці засоби включають інструменти для швидкого реагування на інциденти, а також для оперативного управління загрозами.

5.1. Інструменти моніторингу та аналізу безпеки

Вони дозволяють відстежувати поведінку користувачів та мережеву активність, виявляти аномалії і потенційні загрози.

5.2. План реагування на інциденти

Це набір заходів, які мають бути реалізовані для усунення наслідків інциденту, відновлення роботи систем і захисту від повторення атак.

6. Засоби психологічної ІБ

Засоби психологічної безпеки спрямовані на підвищення обізнаності співробітників щодо інформаційних загроз, зокрема з боку соціальної інженерії та фішингу.

6.1. Тренінги з ІБ

Такі тренінги допомагають співробітникам розпізнавати загрози, навчитися правильно поводитися в разі атаки, наприклад, при отриманні підозрілих електронних листів.

6.2. Мотивація до дотримання стандартів безпеки

Використання різних форм мотивації для заохочення співробітників дотримуватися політик безпеки, включаючи бонуси або штрафи.

Засоби ІБ складаються з різноманітних елементів, що охоплюють технологічні, організаційні, правові та фізичні аспекти. Всі вони повинні діяти в комплексі для забезпечення належного рівня захисту від загроз і мінімізації ризиків у різних сферах[37,с.78].

РОЗДІЛ 2. ЗАСОБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ДЕРЖАВНОГО УПРАВЛІННЯ

2.1 Органи державного управління

Суб’єкти державного управління. Будь-яка соціальна система розглядається в сукупності двох невід'ємних компонентів - суб'єкта і об'єкта. Управлінський вплив суб'єктів здійснюється по відношенню до об'єктів державного управління.

Питаннями державного управління займаються не тільки органи державної влади, а й їх управлінський склад, вони і є суб’єктами. Головною особливістю питання державного управління є наявність певної компетенції та повноважень, що дозволяють йому втілювати свою волю у вигляді управлінських рішень, розпоряджень управління, які є обов'язковими для виконання. Вплив влади, що виходить від суб'єкта на об'єкт управління, дає можливість підпорядкувати волю і діяльність останнього волі першого, що є необхідною умовою для досягнення поставлених цілей і вирішення завдань, що визначаються об'єктом управління. Відповідно об’єкт державного управління зобов’язаний підкорятися владній волі суб’єкта і в обов’язковому порядку виконувати його рішення[41,с.158].

Суб’єкт управління - це система, наділена певною компетенцією і державними повноваженнями, що дозволяють їй втілювати свою волю у вигляді обов'язкових для виконання адміністративних наказів або рішень, тобто це система управління.

З точки зору європейського підходу (моделі) до органів публічного управління належать: органи державної влади (уряд, міністерства, інші центральні органи виконавчої влади, місцеві державні адміністрації); керівник і керівництво цих органів (політики; чиновники; посадові особи, яким делеговано державні повноваження). З точки зору американського

підходу (моделі), питання державного управління включають в себе всі органи і глав трьох гілок влади - законодавчої, виконавчої та судової.

Кожен суб'єкт управління має певні функції, що відображають розподіл праці по всій системі по відношенню до їх виконання, в зв'язку з чим функції характеризують основний зміст і напрямки діяльності об'єкта управління. Суб'єкт організований систематично і в цій якості має характерні риси будь-якої соціальної системи. Для органів управління характерні загальні функції і завдання, єдність їх формування, принципи побудови і діяльності, структурна єдність та інші ієрархічні відносини і відносини, прийняття чітко регламентованих управлінських рішень, узгодження між ними[30,с.80].

Об’єкти державного управління.

Основними об’єктами державного управління відповідно до європейського підходу слід вважати підпорядковані органам виконавчої влади, сектори державного управління, промисловість, державні установи, агентства та суб'єкти господарювання, підпорядковані органам виконавчої влади. Отже, об’єкти державного управління - це система, за допомогою якої спрямовується вплив органів управління. Безпосередніми об'єктами, яких торкається те чи інше конкретне питання, є підгалузі (галузі) державного управління. При більш широкому, американському, підході об'єктами державного управління є все суспільство і будь-які його сфери, галузі, відносини.

Об’єкт управління – це система, яка підпорядковується владній волі суб’єкта управління і виконує його рішення, тобто система, якою управляють.

Слід зазначити, що між суб’єктом і об’єктом управління в системі виконавчої влади не існує абсолютних меж: система, яка управляє, будучи суб’єктом відносно того чи іншого об’єкта, сама, у свою чергу, може бути об’єктом управління з боку іншого суб’єкта. Так, наприклад, обласна державна адміністрація, яка здійснює виконавчу владу в межах регіону, управляється по відношенню до обласних державних адміністрацій

відповідної області, а водночас управляється по відношенню до уряду, який, у свою чергу, здійснює керівництво Президента України та Верховної Ради України[40,с.61].

Необхідно підкреслити визначальне значення об'єкта в системі управління і відносне тлумачення мети самого державного управління. У демократичній, правовій, соціально орієнтованій державі державне управління і, зокрема, державне управління мають на меті забезпечення прав і свобод людини, високої якості життя громадян та безпеки їх існування. Тому така ключова особливість функцій такого управління, як постійна орієнтація на життєво важливі потреби об'єкта, тобто діяльність кожного конкретного суб'єкта повинна аналізуватися з точки зору фактичного забезпечення, перш за все, тих, а не будь-яких інших внутрішніх потреб самого суб'єкта.

Організаційна структура управління - це форма організації системи управління, яка визначає сукупність стійких зв'язків системи, забезпечує її цілісність і ідентичність в собі, тобто збереження основних властивостей при різних внутрішніх і зовнішніх відносинах. Спосіб організації та взаємодії елементів системи та зв'язків між ними є певною особливістю процесів, що відбуваються між елементами системи.

Зовнішнім відображенням організаційної структури управління є склад, мова, розміщення і взаємозв'язок окремих підсистем організації. Вона спрямована, перш за все, на встановлення чітких взаємозв'язків між окремими підрозділами організації, розподіл між ними прав і обов'язків[40,с.107].

В адміністративній структурі кожної організації виділяють такі елементи: ланки, рівні управління і зв'язки - горизонтальні і вертикальні. До ланок управління відносяться структурні підрозділи, а також окремі працівники, які виконують відповідні управлінські функції або їх частину. Зв'язки, що створюються між одношаровими агрегатами, є горизонтальними. Під управлінським шаром розуміють сукупність ланок управління, що

займають певний рівень в системі управління організацією. На одному рівні відбувається розподіл обов'язків між відділами.

Організаційна структура державного управління - це складова системи державного управління, що визначається її соціально-політичним характером, соціально-функціональною роллю, цілями і змістом, яка об'єднує певну сукупність державних організацій, їх кадрові, матеріальні та інформаційні ресурси, що виділяються і витрачаються суспільством на формування і здійснення управлінських впливів держави і підтримання стійкості власних суб'єкт управління[9,с.129].

Органи державної влади, що характеризуються однаковим організаційно-правовим статусом і однорідністю виконуваних управлінських функцій, визначаються поняттям зв'язку в системі державного управління (міністерства, інші центральні органи виконавчої влади, місцеві державні адміністрації тощо).

Системним елементом організаційної структури є державна влада, пов'язана з формуванням і здійсненням державних і розпорядчих впливів. Це єдина владна структура, формально створена державою для реалізації своїх цілей і функцій. У державі, в якій конституційний розподіл влади встановлюється по горизонталі і вертикалі, організаційна структура державного управління набуває певну конфігурацію.

Наступним елементом, що формує організаційну структуру, є організаційні відносини між суб'єктами і об'єктами управління [28,с.110].

В організаційній структурі державного управління виділяють три типи зв'язків:

1. субординаційні (упорядкування згори донизу, від керуючого до керованого);

2. координаційні (упорядкування на одному рівні, між двома і більше суб’єктами, що не виключає того, що загалом вони можуть перебувати на різних рівнях в ієрархічно організованій системі управління);

3.реординаційні (знизу вгору, від керованого до керуючого).

Субординаційні зв’язки в організаційній структурі державного управління можуть передбачати:

1. виключну компетенцію вищого за організаційно-правовим статусом органу щодо органу, нижчого за статусом;

2. безпосереднє і пряме лінійне підпорядкування;

3.функціональне або методичне підпорядкування;

4. право затвердження проекту рішення;

5. підконтрольність;

6. підзвітність.

Координаційні зв’язки базуються на взаємній зацікавленості різних органів державної влади (та органів місцевого самоврядування) в узгодженні своїх управлінських впливів або на один і той самий об’єкт, або на різні об’єкти й можуть передбачати:

1. створення й функціонування спеціальних координаційних органів управління;

2.проведення координаційних нарад;

3.регулярний обмін інформацією, насамперед плановою й обліковою;

4. прийняття одночасних спільних рішень.

Порядок відповідальності органів, що мають між собою координуючі зв'язки (або елементів державного апарату і елементів державного апарату взагалі), може бути передбачений як нормативними рішеннями вищестоящих органів щодо організаційно-правового статусу, так і спільним рішенням[31,с.72].

Спільними рисами є те, що як підпорядковані, так і координаційні відносини в системі виконавчої влади є управлінськими, а також те, що ці відносини можуть існувати як по горизонталі, так і по вертикалі, при наявності різних видів підпорядкування і не тільки організаційних. Спосіб, яким органи виконавчої влади досягають кінцевого результату, різний, як і те, що в координаційних відносинах, на відміну від підпорядкування, сторони виступають як би партнерами.

Відносини перевизначення у виконавчій системі відрізняються від відносин залежності за низкою ознак, а саме: у відносинах залежності управлінський вплив здійснює суб'єкт управління по відношенню до об'єкта управління, а в регулювальних відносинах – об'єкт управління по відношенню до суб'єкта господарювання; координаційні відносини можуть існувати незалежно від підлеглих відносин, оскільки їм не обов'язково повинен передувати управлінський вплив з боку господарського суб'єкта; Здійснення управлінського впливу на залежні відносини є обов'язком господарюючого суб'єкта, а в координаційних відносинах застосування зворотного впливу може бути як правом керованого об'єкта, так і обов'язком суб'єкта господарювання.

Реординаційні зв’язки передбачають:

1. певнусамостійність нижчого за організаційно-правовим статусом установи (у певному колі питань орган приймає рішення без свого попереднього узгодження з органом, що має вищий за організаційно-правовим статусом, і останній може скасувати або призупинити дію цих рішень);
2. право законодавчої, а також нормотворчої ініціативи;
3. право планово-бюджетної ініціативи;
4. право структурно-штатної ініціативи;
5. право представлення для призначення на посаду;
6. право органу, нижчого за організаційно-правовим статусом, брати участь у підготовці рішень органу, вищого за статусом;
7. право органу, нижчого за організаційно-правовим статусом, на консультативне погодження з ним підготовленого вищим органом проекту рішення;
8. право й обов’язок не виконувати незаконний, особливо злочинний наказ.

Організаційна структура є одним з основних елементів управління організацією. Для нього характерний розподіл цілей і завдань управління між підрозділами і співробітниками організацій.

Управлінські організаційні структури відрізняються великою різноманітністю форм. В управлінській практиці найбільш широко використовуються управлінські структури, які називають ієрархічними або бюрократичними[16,с.89].

В ієрархічній структурі організації ті рівні управління, які відображають її продуктивну і економічну структуру, утворюють лінійну організаційну структуру управління.

Необхідність збору, обробки та використання інформації, встановлення зв'язків, забезпечення виробничої та господарської діяльності призвела до появи в системі управління функціональних служб (штаб-квартир), які складають функціональну організаційну структуру управління.

Види організаційних структур

Сукупність лінійних і функціональних органів утворює організаційну структуру управління. Таким чином, організаційні структури управління поділяються на: лінійні, функціональні та комбіновані.

Результатом поєднання лінійних і функціональних структур з іншими критеріями цілей організацій стало виникнення і використання в практиці управління організацією таких структур: продуктова, споживча, територіальна, раціональна бюрократія, відомча, кадрова лінія, функціональна лінія, бюрократична, проектна, матрична, цільова програма, конгломерат та ін.

Лінійна організаційна структура складається з взаємно підлеглих органів у вигляді ієрархії, в якій кожен директор підпорядкований єдиному керівнику, а всі зв'язки з більш високими рівнями управління відбуваються через нього. Переваги структури: простота, зрозумілість і ясність взаємовідносин між зв'язками і керівниками. Недоліки: може

використовуватися тільки у відносно простих організаціях зі стабільними умовами, завданнями та функціями управління.

Функціональна організаційна структура передбачає чітку ієрархію відомчих органів управління, що забезпечують виконання конкретних функцій управління на всіх рівнях. Плюси: менеджери спеціалізуються на окремих адміністративних функціях, які виконують фахівці. Недоліки: процес управління поділяється на сукупність окремих слабо пов'язаних між собою підфункцій з появою неузгоджених дій і повторення.

При лінійних керівниках створюються штаби (служби), які спеціалізуються на виконанні конкретних адміністративних функцій. Вони не мають права приймати рішення, а лише в рамках покладених на них завдань розробляють положення, що забезпечують підготовку якісних управлінських рішень, прийнятих і доручених для виконання керівником. Недоліком є тенденція до збільшення чисельності і розширення кадрових служб.

Відповідно до лінійно-функціональної організаційної структури функціональні служби уповноважені на управління роботою служб нижчого рівня, які виконують певні специфічні функції. При цьому делегуються не лінійні, а функціональні повноваження[10,с.98].

На початку XX ст. Німецький соціолог Макс Вебер (1864-1920) запропонував поняття бюрократії як різновиду нормативної моделі - ідеалу, назвавши її моделлю раціональної (традиційної) бюрократії. Для даної моделі характерні такі особливості:

1. чіткий поділ праці, що забезпечує формування висококваліфікованих спеціалістів;

2. ієрархічність рівнів управління, за якої нижчий рівень контролюється вищим;

3. наявність взаємопов’язаної системи формальних правил і стандартів;

4. формальна безособовість, згідно з якою офіційні особи виконують свої обов’язки;

5. домінування кваліфікаційних вимог під час формування штатів організації.

Недоліками цієї моделі є негнучкість, неадекватне реагування на нові рішення, консервативне ставлення до змін, конфліктність.

Сегментарні організаційні структури використовуються в організаціях з широким асортиментом товарів (послуг), в яких споживачі швидко змінюються, а також в міжнародних організаціях. Серед розділяючих виділяють організаційні структури продукції, споживачів і територіальних організацій.

Споживча організаційна структура утворюється підрозділами, діяльність яких орієнтована на певні групи споживачів (покупців, клієнтів)[36,с.103].

Територіальна організаційна структура формується за географічним розташуванням підрозділів організації у різних регіонах світу, держави чи її регіонів.

Існує чотири основних типи адаптивних організаційних структур: проектні, матричні, програмно-цільові, координаційні. Ці структури здатні швидко пристосовуватись до змін у ринковому оточенні.

Проектні організаційні структури створюються для реалізації конкретних завдань (проектів) з виключною спрямованістю зусиль команди на даний проект.

Матричні групи - це тимчасові групи, члени яких підпорядковуються як керівнику групи (проекту), так і керівникам функціональних відділів, де вони працюють на постійній основі.

Цільова програма – керівник постійно підлаштовується під нові умови, цілі та завдання, що ставляться перед командою для реалізації цільових програм, які можуть змінюватися.

Координаційні - використовуються в умовах одночасного виконання значної кількості програм, в яких функції керівників покладаються на кураторів послуг або їх блоки.

Організаційна структура різнорідної діяльності формується шляхом об'єднання різних типів організаційних структур за рахунок використання останніх в різних службах.

У менеджменті широко використовуються принципи формування раціональної структури організації. Основою цих принципів є принцип примату стратегії над структурою, сформульований А. Чандлером і передбачає, що "стратегія визначає структуру", тобто проектування структури повинно ґрунтуватися на стратегічних планах організації і структура організації повинна забезпечувати виконання цих планів.[43,с.120]

Виходячи з цього, необхідно сформулювати основні цілі держави, побудувати дерево його цілей, виділити важливі і важливі функції, необхідні для досягнення основних цілей держави, і сформувати певні державні органи для їх реалізації. Визначення обсягу цілей державного управління, сукупності основних функцій, виділення з них відокремлених підфункцій – все це фактори, що впливають на вибір структури органів публічної влади. Їх формування здійснюється методами організаційного планування і вимагає врахування закономірності стабільності організацій, що на практиці вимагає прагнення до прийнятного спрощення організаційних структур. З Завжди слід пам'ятати, що їх надмірне ускладнення може призвести до порушення стабільності організації, наростання протиріч між структурними елементами і реальної втрати управління її окремими зв'язками.

2.2 Засоби безпеки в органах державного управління

ДУНБ є специфічною та важливою складовою загальної системи державного управління, яке охоплює всі основні сфери життєдіяльності суспільства та держави — соціальну, економічну, гуманітарну та політичну. Цей процес являє собою цілеспрямовану діяльність органів і суб’єктів забезпечення національної безпеки, що здійснюється в межах чинного

законодавства за допомогою різних можливостей держави, таких як дипломатичні, воєнні, економічні, інтелектуальні та інформаційні ресурси.

Основною метою ДУНБ є ефективне прогнозування, своєчасне виявлення, запобігання та нейтралізація загроз, які можуть поставити під загрозу сталий розвиток людини, суспільства і держави, а також їх життєво важливі інтереси. Важливо, що з організаційно-функціональної точки зору, система ДУНБ є невід'ємною частиною загальної системи державного управління. Її принциповою особливістю є інтеграція з іншими сферами управлінської діяльності, що дозволяє забезпечити комплексний підхід до національної безпеки.

Національні інтереси, а також загрози їх реалізації, охоплюють усі сфери життєдіяльності суспільства та держави. Відповідно, управлінські рішення, які приймаються суб’єктами забезпечення національної безпеки, мають значний вплив на всі аспекти державного управління, включаючи адміністративне, політичне та соціально-економічне управління. Тому ці рішення мають стратегічне значення, часто вирішальне для стабільності та розвитку держави, особливо коли йдеться про нейтралізацію загроз життєво важливим національним інтересам[33,с.99].

У зв’язку з цим, система ДУНБ характеризується як міжгалузеве та функціональне управління. Вона вимагає координації та інтеграції дій різних органів влади, що діють у різних сферах, для забезпечення національних інтересів. Стратегічний напрямок ДУНБ та її ефективність визначаються також формою державного устрою, політичною системою та загальною державною політикою щодо національної безпеки. Важливим є здатність органів ДУНБ швидко адаптуватися до змінюваних умов і забезпечувати належний рівень безпеки на всіх рівнях управління.

ДУНБ є безпосередньо пов’язаним з підтримкою належного рівня захищеності життєво важливих національних інтересів, що, в свою чергу, є основною передумовою розвитку особи, суспільства та держави. Головною метою цього управління є забезпечення стабільності та здатності держави

ефективно реалізувати свої національні інтереси на міжнародній арені, нейтралізуючи загрози, що можуть послабити її роль як суб'єкта міжнародних відносин.

ДУНБ здійснюється на основі чітко визначених нормативних актів, концепцій, стратегій, програм та інших керівних документів, які визначають основні напрямки і завдання в сфері національної безпеки. Ці документи дозволяють державі систематично координувати свої зусилля для створення умов, які забезпечують розвиток країни та захист її інтересів на різних рівнях. Успішна реалізація політики в цій сфері є гарантією стабільності як у внутрішньому розвитку держави, так і в її взаємодії на міжнародній арені[38,с.106].

Суб'єктами, що утворюють систему ДУНБ є посадові особи, органи

1. державного управління, органи місцевого самоврядування,
2. державні інститути,
3. діяльність яких прямо чи опосередковано пов'язана із забезпеченням національної безпеки.

В Україні це, зокрема:

1. Президент України;
2. Верховна Рада України;
3. Кабінет Міністрів України;
4. Рада національної безпеки і оборони України;
5. міністерства та інші центральні органи виконавчої влади;
6. Національний банк України; суди загальної юрисдикції;
7. прокуратура України;
8. місцеві державні адміністрації та органи місцевого самоврядування;
9. вище керівництво збройних сил, спеціальних служб, інших військових формувань, утворених відповідно до чинного законодавства.

Аналіз чинного законодавства України показує, що управлінські впливи суб'єктів ДУНБ спрямовані на різноманітні важливі сфери, які є

основою стабільного розвитку держави та захисту її інтересів. Зокрема, предметами управлінських впливів є:

1. Конституційні права і свободи людини і громадянина — забезпечення прав і свобод громадян є основою демократичного розвитку держави та гарантією її стабільності.

2. Духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності суспільства — це стосується збереження та розвитку культурного спадку, духовних і моральних основ суспільства, що є важливими для національної ідентичності та цілісності держави.

3. Конституційний лад, суверенітет, територіальна цілісність і недоторканність — управлінські впливи спрямовуються на збереження основних принципів державної безпеки, захист суверенітету та територіальної цілісності країни.

4. Інформаційне і навколишнє природне середовище — важливим аспектом є захист інформаційної безпеки та екологічної стабільності, що є необхідним для збереження національної безпеки та сталого розвитку країни.

5. Природні ресурси — управлінські впливи також спрямовуються на ефективне використання та збереження природних ресурсів, що є важливим для економічної безпеки та розвитку держави.

Таким чином, управлінські впливи в сфері національної безпеки охоплюють різноманітні аспекти, які є критичними для стабільності та розвитку держави, а також для забезпечення її внутрішньої та зовнішньої безпеки[35,с.100].

З огляду на це, до опосередкованих об’єктів національної безпеки належать такі важливі аспекти, як життя та власність громадян, а також соціальні, територіальні, етнічні, язикові, релігійні та інші групи, включаючи сім’ю, національні меншини та інші соціальні групи. Для України особливо важливим є право цих груп на організацію та можливість самостійно вирішувати питання групової ідентичності, що в контексті

мультикультурності та різноманіття є важливою складовою національної безпеки.

Вибір конкретних методів та засобів впливу на ці об’єкти управління з боку суб’єктів ДУНБ є результатом необхідності своєчасного і адекватного реагування на загрози національним інтересам. Такий вибір залежить від характеру й масштабу загроз, а також від реальних можливостей, що є у держави або можуть бути сформовані в перспективі. Це включає організаційні, економічні, адміністративні, політичні та інші засоби, які дозволяють ефективно реагувати на виклики та зміцнювати національну безпеку[26,с.23].

Аналіз повноважень суб’єктів державного управління в сфері національної безпеки підтверджує, що забезпечення належної безпеки суспільства і держави є основною передумовою їх життєдіяльності та цілісності. Це підтверджує важливість національної безпеки як одного з основних аспектів функціонування держави. Специфіка методів, сил і засобів, які використовуються для досягнення цієї мети, вказує на те, що ДУНБ є невід’ємною складовою вищого рівня адміністративно-політичного управління.

Ієрархія управління в сфері ДУНБ складається з кількох рівнів:

1. Стратегічний рівень включає органи, які визначають загальний курс і політику в сфері національної безпеки, такі як Верховна Рада України, Президент України, Кабінет Міністрів України та Рада національної безпеки і оборони України (РНБО).
2. Оперативно-стратегічний рівень: охоплює міністерства та відомства, які реалізують національну безпеку через конкретні політики та стратегії.
3. Оперативний рівень: включає державні адміністрації, які здійснюють безпосереднє виконання управлінських функцій на місцевому рівні.

Таким чином, ДУНБ є неперервним процесом, що включає суб’єкт-об’єктні відносини, де здійснюється виконання управлінських функцій,

спрямованих на реалізацію національних інтересів та забезпечення національної безпеки.

Дійсно, політичні, економічні, ідеологічні та інші аспекти життєдіяльності суспільства і держави повинні бути враховані в управлінських рішеннях, прийнятих суб’єктами ДУНБ. Це підкреслює важливість комплексного підходу до національної безпеки, який охоплює всі ключові сфери суспільного та державного життя.

Одним з основних завдань є отримання та ґрунтовний аналіз інформації щодо захищеності від загроз і умов функціонування об’єктів управління. Це дозволяє своєчасно оцінювати ситуацію, передбачати можливі загрози та коригувати стратегії для їх нейтралізації. Оскільки загрози національній безпеці можуть бути різноманітними та змінюватися в динаміці, ефективне управління безпекою потребує постійного моніторингу і аналізу актуальної інформації.

Специфіка ДУНБ полягає в тому, що його функції охоплюють всі сфери життєдіяльності суспільства і держави, що робить цей процес всебічним і важливим для сталого розвитку країни[29,с.80].

Визначення сфери управлінських впливів ДУНБ залежить від обраного підходу до цієї проблеми, і може бути представлене через два основних підходи: "широкий" і "вузький".

1. "Широкий" підхід: Цей підхід є характерним для тоталітарних або авторитарних систем, де державне управління національною безпекою охоплює практично всі сфери життя держави та суспільства. В рамках такого підходу ДУНБ фактично зливається з загальним державним управлінням. У цьому випадку навіть незначні управлінські рішення або дії чиновників розглядаються як сприяння національній безпеці, або, навпаки, як її загроза при неналежному виконанні службових обов'язків. Такий підхід може бути виправданим у періоди війни, надзвичайного стану чи інших кризових ситуацій, коли необхідна концентрація ресурсів і владних повноважень для збереження національної безпеки.

2. "Вузький" підхід: Згідно з цим підходом, сфера ДУНБ обмежується тільки тими функціями, які сприяють створенню належних умов для забезпечення життєво важливих національних інтересів, і реалізації конкретних заходів, необхідних для підтримки стабільності держави. Цей підхід ставить акцент на ефективному та цілеспрямованому використанні управлінських повноважень у конкретних сферах, що мають пряму відношення до безпеки держави, таких як оборона, боротьба з тероризмом, захист інформаційного середовища тощо. Водночас розмежування функцій ДУНБ та інших сфер управління дозволяє уникати надмірної концентрації влади та зловживань.

Ці два підходи відображають різні філософії державного управління, що визначають, наскільки широко або вузько мають бути розширені повноваження органів, які займаються національною безпекою. Однак для ефективного функціонування системи національної безпеки важливо знаходити баланс між цими підходами, враховуючи об'єктивні умови та реальні загрози національним інтересам.

2.3 Вплив діяльності органів державного управління на інформаційну безпеку України

Державне регулювання є складним соціальним, правовим і політичним феноменом. Воно передбачає приведення поведінки суб'єктів та їхніх утворень до дотримання вимог правових норм, а також обмеження поведінки через дозволи та заборони. Таке регулювання завжди здійснюється через застосування права в межах управлінського процесу. Специфіка сфери суспільних відносин, що підлягає регулюванню, визначає вибір оптимальних юридичних інструментів, з урахуванням стандартів прав людини та громадянина.

Сфера забезпечення ІБ є особливо важливою, адже, незважаючи на певну нормативну невизначеність терміну «інформаційна безпека», чинна Конституція України від 28 червня 1996 року визнає забезпечення ІБ однією з найважливіших функцій держави і справою всього українського народу. Реалізуючи це положення, держава формує окремий напрям внутрішньої політики, спрямований на забезпечення ІБ України[23,с.154].

Враховуючи специфіку державного управління у сфері забезпечення інформаційної безпеки держави, під правовими формами державного регулювання у цій сфері можна розуміти визначені чинним законодавством види юридично значущої діяльності уповноважених суб'єктів державного управління. Ці форми регулювання включають процеси запобігання, припинення та ліквідації наслідків посягань на ІБ України. Застосування таких форм має наслідки, що змінюють правове становище учасників відносин у сфері забезпечення ІБ або впливають на національне інформаційне середовище.

Зокрема, правовими формами є видання нормативних та індивідуальних актів, що стосуються реалізації державної політики у сфері забезпечення ІБ, а також здійснення інших юридично значущих дій, пов'язаних з інформаційними відносинами.

Основне призначення нормативних та індивідуальних актів у сфері Іб полягає в створенні системи норм, які встановлюють правовий режим забезпечення її як соціально-державної цінності та деталізують загальні положення законодавства щодо протидії інформаційним загрозам. Так, норми Закону України «Про національну безпеку України» від 21 червня 2018 року визначають, що забезпечення ІБ є складовою частиною національної безпеки. Відповідно, суб'єкти, уповноважені здійснювати державне управління у сфері ІБ, видають підзаконні нормативні та індивідуальні акти для стратегічного і оперативного впливу на процеси функціонування національного інформаційного простору.

Видання нормативних актів як правова форма державного управління у сфері забезпечення ІБ має свої особливості. Зокрема, нормативні акти можна класифікувати на акти універсальної дії, спеціальної дії та локальної дії[15,с.90]:

1. Акти загальної дії: ці акти поширюють регуляторний вплив на всі органи та установи, які залучені до реалізації державної політики у сфері забезпечення ІБ.

2. Акти спеціальної дії: ці акти діють лише на конкретні органи, наприклад, Службу безпеки України, чи на певні установи, як-от Міністерство закордонних справ.

3. Акти локальної дії: вони мають регулятивне значення лише на рівні конкретного органу чи установи, яка уповноважена здійснювати завдання з забезпечення інформаційного суверенітету держави.

Яскравим прикладом такого нормативного акта є Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", яке було введено в дію Указом Президента України від 25 лютого 2017 року.

Зазначений документ створює адміністративно-правову основу для виконання важливих завдань у сфері забезпечення ІБ держави. В його положеннях зазначено основні загрози інформаційній безпеці України, а також визначено перелік органів державної влади, які, здійснюючи співробітництво, розробляють та реалізують завдання в цій сфері. Зокрема, це включає Міністерство інформаційної політики України (до реорганізації в 2019 році), Міністерство закордонних справ, Міністерство оборони, Міністерство культури, СБУ, розвідувальні органи, Державну службу спеціального зв’язку та захисту інформації.

Документ також формулює пріоритетні напрямки державної політики для кожного з цих відомств, а також встановлює нормативні засади координації між ними. Рада національної безпеки і оборони України, як дорадчий орган при Президентові України, і Кабінет Міністрів України, який

здійснює загальну інформаційну політику, є основними координуючими інституціями.

Доктрина також покладає певні спеціальні обов'язки та надає повноваження суб’єктам державного управління. Наприклад, на СБУ покладається здійснення моніторингу спеціальними методами та способами вітчизняних і іноземних ЗМІ та Інтернет-ресурсів з метою виявлення загроз національній безпеці в інформаційній сфері[21,с.89].

Проте, на даний момент в правовій системі України не існує чітких нормативних актів, які б регламентували співробітництво суб'єктів державного управління, уповноважених виконувати функції забезпечення інформаційної безпеки держави.

Правові акти індивідуальної дії в сфері забезпечення інформаційної безпеки спрямовані на врегулювання конкретних ситуацій, що виникають у цій сфері. Вони можуть бути спрямовані на окремих суб’єктів або визначати певний режим зберігання, використання чи захисту інформації. Такі акти мають більш точне і обмежене застосування порівняно з нормативними актами загальної чи спеціальної дії.

Яскравим прикладом є положення Закону України «Про державну таємницю» від 21 січня 1994 р. № 3855-XII, яке регулює видання наказів щодо призначення осіб на посади, що відповідають за режим секретності, таких як заступники керівників з питань режиму, начальники режимно-секретних органів та їхні заступники. Також такі акти можуть визначати обов’язки окремих працівників щодо забезпечення секретності, зокрема через накази чи інші індивідуальні правові акти.

Не менш важливим аспектом у сфері забезпечення інформаційної безпеки є здійснення інших юридично значущих дій, які спрямовані на регулювання процесів збирання, використання та поширення інформації. Юридично значущі дії розглядаються як діяльність, що здійснюється на основі законів та підзаконних актів, і мають конкретні юридичні наслідки,

такі як державна реєстрація, видача офіційних документів, ліцензування або складання адміністративного протоколу.

Прикладом такої юридично значущої дії є віднесення інформації до категорії, що має режим державної таємниці. Наприклад, Наказ СБУ «Про затвердження Зводу відомостей, що становлять державну таємницю» від 12 серпня 2005 р. № 440 визначає, що СБУ має монопольне право формувати Звід відомостей, що становлять державну таємницю, і здійснювати реєстрацію відповідної інформації в цьому Зводі. Ця інформація має особливий статус і підлягає обмеженому доступу для запобігання її публічному розголошенню. Внесення інформації до Зводу є юридичним фактом, який спричиняє виникнення, зміну або припинення адміністративно-правових відносин у сфері захисту такої інформації. Це є результатом управлінського рішення, яке має значущі правові наслідки для осіб, відповідальних за збереження та обробку цієї інформації[8,с.87].

Окрім вищезазначених правових дій, важливим прикладом юридично значущих дій є складання протоколів про адміністративні правопорушення, що посягають на інформаційну інфраструктуру України та режим використання інформації загалом. Складання протоколу є формальною підставою для притягнення винної особи до адміністративної відповідальності. Адміністративна відповідальність є важливим механізмом правового впливу на сферу ІБ поряд із кримінальною відповідальністю, оскільки вона охоплює значний обсяг суспільних відносин в інформаційній сфері.

Єдиним кодифікованим законодавчим актом, що містить склади адміністративних правопорушень у цій сфері та визначає заходи адміністративної відповідальності, є Кодекс України про адміністративні правопорушення від 7 грудня 1984 року. Цей кодекс передбачає відповідальність за порушення, що стосуються захисту інформаційної інфраструктури та регулювання використання інформації, що є важливою складовою державної політики у сфері ІБ.

Слід підкреслити, що чинний Кодекс України про адміністративні правопорушення передбачає адміністративну відповідальність за порушення в сфері інформаційних відносин у різних галузях. Зокрема, відповідальність за порушення у таких сферах:

- охорона праці та здоров'я населення (ст. 41-3);
- охорона природи, використання природних ресурсів, охорона культурної спадщини (ст. ст. 53-2, 82-1, 82-3, 91-4, 92-1);
- шляхове господарство та зв'язок (ст. ст. 116-3, 144, 145, 148);
- житлово-комунальне господарство та благоустрій (ст. 149-1);
- господарська діяльність та послуги (ст. ст. 163-5, 163-9, 163-11, 164-6, 164-9, 166-4);
- протидія корупції (ст. 172-8);
- порядок управління (ст. ст. 184-2, 185-11, 186-3, 188-7, 188-31, 188-32, 188-35, 188-36, 188-37, 188-39, 211-2, 211-5, 2012-2, 212-3, 212-5, 212-6);
- здійснення народного волевиявлення та забезпечення порядку його проведення (ст. ст. 212-7, 212-8, 212-9, 212-11, 212-13, 212-14).

Таким чином, адміністративна відповідальність є важливим механізмом гарантування інформаційного правопорядку в державі, забезпечуючи дотримання законності в інформаційних відносинах і попереджаючи можливі порушення, що можуть шкодити національним інтересам та безпеці.

Проаналізовані правові форми державного регулювання у сфері забезпечення ІБ України є надзвичайно різноманітними за змістом та володіють значним регуляторним потенціалом, що робить їх важливим чинником національної безпеки держави. Однак їх ефективність на практиці значною мірою залежить від рівня професійної підготовки працівників органів державного управління, відповідальних за здійснення владних дій у сфері забезпечення ІБ.

При цьому зміст правових форм регулювання завжди повинен відповідати рівню розвитку технологій, методів та інструментів, що використовуються для створення загрози національному інформаційному середовищу. Тому важливим перспективним напрямом наукових досліджень є формулювання науково обґрунтованих пропозицій щодо оптимізації регулювання правових форм державного управління у цій сфері з урахуванням організаційних та технічних аспектів. Це дасть змогу ефективніше реагувати на інформаційні загрози та забезпечувати належний рівень національної безпеки[45].

Центральним органом, спеціально уповноваженим здійснювати координацію та контроль забезпечення ІБ як складової національної безпеки і оборони в межах компетенції та покладених на нього функцій, є Рада національної безпеки і оборони України, яка, відповідно до своїх повноважень:

1. визначає стратегічні національні інтереси України, концептуальні підходи та напрями забезпечення національної безпеки і оборони в інформаційній сфері;
2. формує проекти державних програм, доктрин, законів України, указів Президента України, директив Верховного Головнокомандувача Збройних Сил України, міжнародних договорів, інших нормативних актів і документів з питань інформаційної безпеки України; координує і здійснює контроль над іншими державними органами сектору національної безпеки і оборони в сфері забезпечення ІБ України;
3. здійснює постійний моніторинг впливу на національну безпеку процесів, що відбуваються в інформаційній сфері;
4. визначає стан інформаційної агресії та звертається до Верховної Ради України з пропозицією про введення спеціального правового режиму захисту інформаційного простору держави.

Основними суб’єктами реалізації державної політики в сфері інформаційної безпеки, в межах їх повноважень та завдань, є:

1. Служба безпеки України;
2. Міністерство внутрішніх справ України;
3. Міністерство оборони України;
4. Служба зовнішньої розвідки України;
5. Центральний орган виконавчої влади із спеціальним статусом, який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій і користування радіочастотним ресурсом України.

Формування, реалізація та координація державної інформаційної політики, а також забезпечення інформаційного суверенітету України здійснюються спеціально уповноваженим центральним органом виконавчої влади відповідно до покладених на нього функцій[50].

Завданнями центрального органу виконавчої влади в сфері державної інформаційної політики є:

1. розробка концептуальних документів в сфері сталого розвитку інформаційного простору та контроль за їх виконанням в системі органів виконавчої влади;
2. координація діяльності центральних органів виконавчої влади щодо забезпечення сталого розвитку інформаційного простору України;
3. участь у формуванні та реалізації стратегій, програм та планів, якими визначаються цільові настанови, принципи і напрями реалізації положень цієї Концепції;
4. підготовка нормативних документів, що регламентують порядок зв'язків з громадськістю органів державної влади та оприлюднення інформації про їх діяльність, а також координація та контроль діяльності підрозділів центральних органів виконавчої влади, що здійснюють комунікацію з громадськістю.

Основними суб'єктами реалізації державної інформаційної політики України є такі центральні органи виконавчої влади, які формують та реалізують державну політику в наступних напрямах:

1. у сферах освіти і науки, інтелектуальної власності, наукової, науковотехнічної та інноваційної діяльності, інформатизації, формування і використання національних електронних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства, а також у сфері здійснення державного нагляду (контролю) за діяльністю навчальних закладів незалежно від їх підпорядкування і форми власності;

2. у сферах культури та мистецтв, охорони культурної спадщини,

вивезення, ввезення і повернення культурних цінностей, державної мовної політики, а також у сфері формування та реалізації державної політики у сфері кінематографії (останнє – це Держкіно);

3. у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства;

4. у сфері телебачення і радіомовлення, інформаційній та видавничій сферах.

Спеціально уповноважений центральний орган виконавчої влади, що здійснює формування, реалізацію та координацію державної інформаційної політики, а також основні суб'єкти реалізації державної інформаційної політики, здійснюють свою діяльність у взаємодії з:

1. постійно діючим колегіальним органом, метою діяльності якого є нагляд за дотриманням законів України у сфері телерадіомовлення, а також здійснення регуляторних повноважень (Національна рада України з питань телебачення і радіомовлення);

2. органом державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв`язку;

3. органами саморегуляції медіасфери України.

РОЗДІЛ 3. ВПЛИВ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РОБОТУ ДЕРЖАВНОЇ СЛУЖБИ ЯКОСТІ ОСВІТИ УКРАЇНИ

3.1 Загальна характеристика діяльності ДСЯО

ДСЯО – це орган виконавчої влади, відповідальний за забезпечення та підтримку високих стандартів якості освіти у закладах освіти України. Основною метою її діяльності є формування системи моніторингу та оцінювання якості освіти, сприяння підвищенню кваліфікації педагогів та покращення навчального середовища. ДСЯО також забезпечує виконання нормативно-правових актів у сфері освіти та здійснює нагляд за дотриманням освітніх стандартів.

Одним із ключових завдань служби є організація інституційних аудитів закладів освіти, які спрямовані на оцінку якості управління та освітнього процесу. Під час аудитів враховуються показники результативності навчання, умови для забезпечення якості освіти, педагогічна майстерність викладачів і задоволеність учасників освітнього процесу. Окрім цього, ДСЯО надає консультації та рекомендації для покращення роботи закладів освіти, допомагаючи адаптувати їх до сучасних викликів і стандартів[17].

ДСЯО також активно взаємодіє з громадськістю, батьками, учнями та педагогами, залучаючи їх до процесу оцінювання освіти. Однією з її функцій є забезпечення прозорості інформації про якість освіти через публікацію результатів досліджень і аудитів. Завдяки цьому ДСЯО сприяє підвищенню довіри до системи освіти України та створенню умов для її подальшого розвитку відповідно до міжнародних стандартів.

Державна служба якості освіти України (далі - Служба) відповідно до Положення про ДСЯО, затвердженого постановою Кабінету Міністрів України від 14 березня 2018 р. № 168, є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів

України через Міністра освіти і науки та який реалізує державну політику у сфері освіти, зокрема з питань забезпечення якості освіти, забезпечення якості освітньої діяльності, здійснення державного нагляду (контролю) за закладами освіти щодо дотримання ними законодавства.

Основними завданнями Служби є: (положення)

1. реалізація державної політики у сфері освіти, зокрема з питань забезпечення якості освіти, забезпечення якості освітньої діяльності, здійснення державного нагляду (контролю) за закладами освіти щодо дотримання ними законодавства, у межах повноважень, передбачених законом;
2. внесення на розгляд Міністра освіти і науки пропозицій щодо забезпечення формування державної політики у сфері освіти з питань, що належать до компетенції Служби.

Служба відповідно до покладених завдань:

1. узагальнює практику застосування законодавства з питань, що належать до її компетенції, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України, нормативно-правових актів міністерств та в установленому порядку подає їх на розгляд Міністра освіти і науки;

2. проводить інституційний аудит закладів освіти;

3. надає рекомендації закладам освіти (крім закладів вищої освіти) щодо організації та функціонування внутрішньої системи забезпечення якості освіти;

4. затверджує за результатами експертизи освітні програми дошкільної та загальної середньої освіти (крім типових і тих, що розроблені на основі типових);

5. проводить моніторинг якості освітньої діяльності та якості освіти у порядку, визначеному законодавством;

6. акредитує громадські фахові об’єднання та інших юридичних осіб, що здійснюють незалежне оцінювання якості освіти та освітньої діяльності закладів освіти (крім закладів вищої освіти), веде їх реєстр;

7. здійснює у межах повноважень, передбачених законом, державний нагляд (контроль) за діяльністю закладів освіти щодо дотримання ними вимог законодавства про освіту та видає обов’язкові до виконання ними розпорядження щодо усунення виявлених порушень у визначені строки;

8. здійснює за дорученням МОН контроль за дотриманням вимог щодо організації зовнішнього незалежного оцінювання;

9. у порядку, визначеному МОН, аналізує діяльність місцевих органів виконавчої влади, органів місцевого самоврядування, їх структурних підрозділів з питань освіти (за наявності) в частині, що стосується дотримання вимог законодавства з питань освіти і забезпечення якості освіти на відповідній території, та надає їм відповідні висновки і рекомендації, що оприлюднюються протягом п’яти робочих днів з дня їх надання на офіційному веб-сайті Служби та відповідного органу виконавчої влади чи органу місцевого самоврядування;

{Підпункт 9 пункту 4 в редакції Постанови КМ № 1222 від 09.12.2020}

9-1) складає у випадках, передбачених законом, протоколи про адміністративні правопорушення;

{Пункт 4 доповнено підпунктом 9-1 згідно з Постановою КМ № 1222 від 09.12.2020}

10. бере участь в розробленні державних стандартів загальної середньої освіти;

11. здійснює контроль за веденням обліку дітей шкільного віку в частині здійснення структурними підрозділами місцевих органів виконавчої влади та органів місцевого самоврядування повноважень, визначених законом;

12. бере участь у сертифікації педагогічних працівників відповідно до закону;

13. здійснює управління об’єктами державної власності, що належать до сфери її управління;

14. здійснює розгляд звернень громадян з питань, що належать до її компетенції;

15. здійснює міжнародне співробітництво з питань, що належать до її компетенції;

16. здійснює інші повноваження, передбачені законом.

Служба з метою організації своєї діяльності:

1. забезпечує в межах повноважень, передбачених законом, здійснення заходів щодо запобігання корупції і контролю за їх реалізацією в апараті Служби та її територіальних органах, на підприємствах, в установах та організаціях, що належать до сфери її управління;
2. організовує планово-фінансову роботу в апараті Служби, її територіальних органах, на підприємствах, в установах та організаціях, що належать до сфери її управління, здійснює контроль за використанням фінансових і матеріальних ресурсів, забезпечує організацію та вдосконалення бухгалтерського обліку в установленому законодавством порядку;
3. забезпечує ефективне і цільове використання бюджетних коштів;
4. організовує ведення діловодства та архівне зберігання документів відповідно до встановлених правил;
5. забезпечує у межах повноважень, передбачених законом, виконання завдань з мобілізаційної підготовки та мобілізаційної готовності держави;
6. забезпечує в установленому порядку самопредставництво в судах та інших державних органах через осіб, уповноважених діяти від її імені, зокрема через посадових осіб юридичної служби або інших уповноважених осіб, а також забезпечує представництво інтересів Служби в судах та інших державних органах через представників.

ДСЯО — це центральний орган виконавчої влади, створений 6 грудня 2017 року. Її діяльність координується Кабінетом Міністрів України через Міністерство освіти і науки України. Основна мета ДСЯО полягає в реалізації державної політики у сфері освіти, зокрема:

1. Забезпечення якості освіти.
2. Забезпечення якості освітньої діяльності.
3. Здійснення державного нагляду та контролю за дотриманням закладами освіти вимог чинного законодавства.

ДСЯО відіграє ключову роль у формуванні стандартів якості освіти, а також в аналізі, оцінці та вдосконаленні освітньої діяльності на всіх рівнях.

Територіальні органи ДСЯО функціонують як юридичні особи публічного права, створені Урядом. Вони охоплюють 24 обласні управління та управління в м. Києві, забезпечуючи реалізацію повноважень Служби на відповідних територіях[19,с.45].

Основна мета територіальних органів— підтримка закладів освіти, їх керівників та педагогічних працівників у підвищенні якості освітньої діяльності та результатів навчання учнів.

Ключовий інструмент оцінювання — інституційний аудит.

Інституційний аудит дозволяє:

1. Проаналізувати якість освітньої діяльності закладу освіти.
2. Надати обґрунтовані рекомендації для вдосконалення роботи школи.
3. Забезпечити підтримку у впровадженні запропонованих змін.

Цей процес спрямований на покращення навчальних результатів учнів та підвищення ефективності управління закладами освіти.

У центральному апараті функціонує відділ інформаційних технологій і управління організаційно-документального забезпечення, який виконує широкий спектр завдань, зокрема:

1. Функції відділу ІТ:

    1. Адміністрування всіх інформаційних систем Служби.

2. Забезпечення кібербезпеки та функціонування системи інформаційної безпеки.
3. Обслуговування та підтримка користувачів інформаційних систем.

2. Функції управління організаційно-документального забезпечення:

1. Адміністрування системи електронного документообігу АСКОД.
2. Виконання налаштувань для роботи системи:
3. Організація обміну інформацією.
4. Формування номенклатур справ.
5. Ведення реєстрації документів.
6. Направлення, додавання адресатів і пересилання документів.

Через відсутність окремого підрозділу, відповідального за ІТ, усі пов'язані з інформаційними технологіями та кібербезпекою обов'язки зосереджені в цьому відділі. Це створює універсальну систему адміністрування, яка забезпечує безперервну та ефективну роботу всіх інформаційних і документаційних процесів[48].

Тому в своїй роботі територіальні органи керуються документами саме Центрального апарату, незалежно від того, що вони є іншими юридичними особами і можуть розробляти свої положення, правила і т.д. Це стосується користування комп'ютерами, програмного забезпечення , електронних пошт, веб сайтів. Також у кожному територіальному органі є свій діловод, який виконує функції адміністратора АСКОД більш нижчого рівня, ніж у центральному апараті. Дана особа може виконувати реєстрацію, перевірки підписів у межах територіального органу.

АСКОД у ДСЯО забезпечує ефективне управління документами та оптимізує діловодство. Вона автоматизує процеси створення, реєстрації, зберігання, розподілу та контролю виконання документів. Завдяки інтеграції електронного документообігу з іншими внутрішніми системами, АСКОД сприяє оперативному доступу до інформації, скорочує час обробки

документів і мінімізує ймовірність помилок, пов’язаних із ручним введенням даних.

Система також підтримує функцію моніторингу виконання завдань та зобов’язань, що дозволяє керівництву ДСЯО контролювати процеси у реальному часі. АСКОД включає можливості електронного підпису, що забезпечує юридичну силу електронних документів і підвищує рівень безпеки. Завдяки використанню цієї системи ДСЯО може більш ефективно взаємодіяти із закладами освіти, іншими державними органами та громадськістю, сприяючи прозорості та підзвітності своєї діяльності.

Для того, щоб забезпечити роботу територіальних органів і служби основна документація проходить саме через АСКОД, який використовується з двома видами ліцензії:

1. іменними – їх 90%; присвоюються до конкретної людини
2. конкурентні – 10%; однією ліцензією можуть користуватися до десяти людей, але тільки один в певний період часу.

Для передачі решти документів використовуються або обмін між робочими станціями або обмін між поштовими скриньками працівників.

3.2 Вплив засобів інформаційної безпеки на роботу ДСЯО

Вплив засобів ІБ на роботу ДСЯО є суттєвим, адже вона є критично важливою для ефективного функціонування організації, яка оперує значними обсягами чутливих даних про заклади освіти, педагогів та учнів. Надійні засоби ІБ дозволяють зберігати конфіденційність даних, захищаючи їх від несанкціонованого доступу, що сприяє підтримці довіри до діяльності служби.

Одним із ключових аспектів впливу є захист персональних даних. ДСЯО працює з інформацією, яка включає результати аудитів, оцінювання педагогів, а також персональні дані учнів та вчителів. Використання

сучасних засобів шифрування та систем управління доступом забезпечує конфіденційність і цілісність цієї інформації. Це не лише відповідає законодавству України, а й допомагає уникнути репутаційних ризиків, пов'язаних із витоками даних.

Другий важливий аспект – це забезпечення безпеки онлайн-комунікацій. У зв’язку з діджиталізацією освітнього процесу та збільшенням обсягів дистанційної роботи, ДСЯО активно використовує електронні платформи для моніторингу, аналізу та взаємодії з закладами освіти. Засоби захисту, такі як брандмауери, антивірусне програмне забезпечення та системи виявлення загроз, мінімізують ризики кібератак та саботажу[46].

Третім аспектом є створення безпечної інфраструктури для зберігання та аналізу даних. Використання хмарних технологій та резервного копіювання дозволяє ДСЯО зберігати важливу інформацію з гарантією її доступності у разі технічних збоїв чи кібератак. Це також сприяє підвищенню ефективності роботи служби, адже дані стають доступними для аналізу та прийняття рішень у реальному часі.

Останній аспект – це підвищення цифрової грамотності працівників. Засоби ІБ вимагають відповідного рівня обізнаності серед персоналу. ДСЯО впроваджує програми навчання та тренінги для співробітників, що знижує ризик людського фактору в загальній системі безпеки. Таким чином, засоби інформаційної безпеки не лише захищають інформацію, а й сприяють вдосконаленню внутрішніх процесів у службі.

Месенджери такі як телеграм або вайбер є забороненими або не рекомендованими для роботи. Тож для функціонування центрального апарату та територіальних органів ДСЯО відділ айті спільно з юристами і документознавцями розробляють правила, інструкції, положення і вимоги по використанню програмного забезпечення, техніки та системи електронного документнообігу, поштових скриньок[додаток 1].

Службова електронна пошта - електронна пошта (поштова скринька) працівника установи, сформована з використанням доменного імені у домені gov.ua для обміну управлінською інформацією, яка не має юридичної сили.

Так як ліцензій не вистачає на територіальні органи служби то іноді обмін проектами документів здійснюється за допомогою електронної пошти між працівниками як центрального апарату так і в межах територіального органу [додаток 3].

Деякі програми може встановлювати лише окремий працівник, у центральному апараті це відділ айті, а в територіальному органі відповідальний працівник призначений керівником управління або сам керівник[додаток 3].

Частина заходів з обміну інформацією вирішуються або технічними або організаційними заходами. Територіальні органи та центральний апарат мають своїх експертів: інституційний аудит, моніторинги, проведення аналізу, заходи нагляду і контролю та сертифікація. Раніше з цими експертами комунікували з використанням месенджерів. Але в зв'язку із їх забороною працівники перейшли на електронну пошту. Для полегшення роботи було розроблено шаблони для швидкої передачі повідомлень та документів. Таким чином працівник може швидко знайти шаблон по необхідній даті або прізвищу працівника та вставивши текст легко передати йому потрібному користувачу або відділу установи [11,с.101].

Засоби інформаційної безпеки відіграють ключову роль у захисті даних, які обробляє ДСЯО. Оскільки служба працює з великими обсягами інформації, зокрема персональних даних учнів, педагогів та освітніх установ, застосування таких засобів, як шифрування та багаторівнева автентифікація, дозволяє мінімізувати ризики витоків або несанкціонованого доступу. Це особливо важливо в умовах цифровізації освіти та зростання кіберзагроз.

ІБ допомагає забезпечити цілісність даних, що передаються або зберігаються в системах ДСЯО. Використання криптографічних методів та регулярних перевірок систем дозволяє запобігти модифікації чи підробці

важливих документів, таких як сертифікати, звіти про якість освіти чи результати перевірок. Це створює умови для об’єктивної оцінки якості освіти.

ДСЯО може стати об'єктом кібератак, спрямованих на порушення роботи систем або маніпулювання інформацією. ІБ забезпечує захист від таких загроз завдяки використанню фаєрволів, систем виявлення вторгнень (IDS) та постійному моніторингу інфраструктури. Це дозволяє зберігати стабільну роботу систем навіть в умовах зовнішнього впливу.

У сучасному світі значна частина роботи ДСЯО виконується у віддаленому режимі або з використанням електронних платформ. Засоби інформаційної безпеки, такі як VPN, цифрові підписи та сертифікати, забезпечують безпечний обмін документами та проведення онлайн-нарад. Це сприяє ефективній роботі служби навіть за умов обмеженого фізичного доступу до офісів[49].

Захищеність інформації є важливим фактором для формування довіри до ДСЯО як серед освітян, так і серед громадськості. Впровадження сучасних засобів інформаційної безпеки демонструє прозорість і надійність роботи служби, що є важливим для суспільного визнання. Надійний захист даних дозволяє уникнути репутаційних ризиків та підтримує високий рівень взаємодії з освітніми закладами.

3.3 Перспективи впровадження новітніх засобів інформаційної безпеки в роботу ДСЯО

ДСЯО оперує величезними обсягами даних, серед яких є персональна інформація учнів, вчителів, адміністрації навчальних закладів, а також результати моніторингів і аудиторських перевірок. Надійні засоби інформаційної безпеки, такі як шифрування даних, біометричні системи доступу та автоматизовані системи аудиту, забезпечують захист інформації від витоку чи маніпуляцій. Захищені бази даних створюють впевненість, що

інформація використовується лише за призначенням і не потрапляє до третіх осіб[12,с.63].

Сучасні загрози, зокрема хакерські атаки, віруси чи фішинг, можуть не лише порушити роботу інформаційних платформ ДСЯО, але й підірвати довіру до установи. Застосування міжмережевих екранів, багаторівневого моніторингу систем та програмного забезпечення з аналізом поведінки користувачів допомагають зменшити вразливість до таких атак. Особливо важливо враховувати виклики гібридної війни, коли зловмисники намагаються отримати доступ до державних даних для підривної діяльності.

ДСЯО активно використовує цифрові платформи для збору, аналізу та публікації даних про якість освіти. Завдяки резервному копіюванню, розподіленим системам зберігання даних і хмарним технологіям, такі платформи залишаються доступними навіть у разі технічних збоїв чи надмірного навантаження. Наприклад, у період масового завантаження даних результатів моніторингу платформи залишаються стабільними завдяки використанню динамічних ресурсів серверів.

Інформаційна безпека не є суто технічною сферою – вона також залежить від обізнаності співробітників ДСЯО. Проведення навчальних семінарів із цифрової безпеки, регулярні тренінги та інструктажі щодо безпечного користування корпоративними системами допомагають мінімізувати ризики, пов’язані з людським фактором. Наприклад, навички розпізнавання шахрайських листів, створення складних паролів та роботи у захищених мережах знижують ймовірність помилок, які можуть призвести до серйозних наслідків.

Засоби інформаційної безпеки створюють базу для прозорості діяльності ДСЯО. Захищені платформи, які унеможливлюють втручання у результати моніторингів, забезпечують довіру освітян, учнів та батьків до системи оцінювання. Наприклад, використання технологій блокчейн може гарантувати, що дані про результати перевірок є автентичними та не можуть бути змінені після їхнього внесення.

Сфера освіти постійно змінюється, і ДСЯО має реагувати на нові виклики, пов’язані з діджиталізацією. Засоби інформаційної безпеки дозволяють розширювати функціонал цифрових інструментів, таких як електронні платформи оцінювання, онлайн-сервіси для навчальних закладів і цифрові документообіги. Наприклад, інтеграція систем штучного інтелекту для аналізу освітніх даних вимагає додаткових рівнів захисту, які забезпечують конфіденційність і точність результатів.

У кризових умовах, наприклад під час військових дій чи техногенних катастроф, стабільність і захищеність систем ДСЯО стають критично важливими. Використання ізольованих серверів, зашифрованих каналів передачі даних та мобільних платформ дає змогу забезпечити безперебійну роботу навіть за складних умов. Це особливо важливо для швидкого реагування на зміни у сфері освіти під час надзвичайних ситуацій [49].

Інформаційна безпека є важливою складовою інтеграції ДСЯО в міжнародний освітній простір. Використання міжнародних стандартів у сфері кібербезпеки дозволяє службі ефективно співпрацювати з іноземними партнерами, обмінюватися даними та брати участь у міжнародних дослідженнях, зокрема PISA. Захищеність інформаційних платформ сприяє довірі партнерів та створює можливості для отримання додаткових ресурсів на розвиток.

ІБ є основою для впровадження сучасних цифрових технологій у сфері освіти. ДСЯО поступово переходить до електронного документообігу, цифрових платформ оцінювання якості навчання та автоматизованих систем збору даних. Захист цих інноваційних рішень забезпечує ефективність роботи служби, знижує витрати на паперову документацію та пришвидшує обмін інформацією. Наприклад, впровадження електронних протоколів перевірок навчальних закладів стало можливим завдяки впевненості у надійності систем зберігання даних[13,с.136].

Не менш важливим аспектом ІБ є захист від внутрішніх загроз, таких як ненавмисні помилки працівників або зловмисні дії всередині установи.

Використання систем журналювання дій користувачів, моніторинг доступу до інформації та впровадження принципів мінімізації прав доступу дозволяє ДСЯО швидко виявляти потенційні ризики. Наприклад, регулярний аналіз логів систем допомагає відслідковувати спроби несанкціонованого доступу або аномальні дії у внутрішніх базах даних.

Робота ДСЯО у сфері ІБ тісно пов’язана із дотриманням законодавства України та міжнародних норм щодо захисту даних. Впровадження засобів інформаційної безпеки враховує вимоги, прописані у законах про захист персональних даних та інформаційні ресурси. Крім того, участь у міжнародних освітніх програмах передбачає відповідність європейським стандартам, таким як GDPR. Це підвищує довіру до ДСЯО на міжнародній арені та сприяє розвитку партнерських зв’язків[47].

У підсумку, засоби ІБ не лише підтримують стабільність роботи ДСЯО, але й сприяють довгостроковому розвитку якісної та прозорої системи освіти в Україні, забезпечуючи її інтеграцію у сучасний цифровий світ.

ВИСНОВКИ

У результаті проведеного дослідження ми дійшли таких висновків.

1. Під час дослідження нами було зроблено огляд наукової літератури стосовно засобів інформаційної безпеки, який показав, що принципи сучасного захисту інформації можна сформулювати як пошук оптимального балансу між доступністю та безпекою. Це означає, що система повинна забезпечувати своєчасний доступ до необхідної інформації, водночас захищаючи її від несанкціонованого доступу чи змін. Важливо знайти таке співвідношення, яке забезпечить високу рівень безпеки без надмірного обмеження доступу до ресурсів, що може вплинути на ефективність роботи системи .

2. Розглянувши сутність поняття «інформаційна безпека» та її засоби ми зрозуміли, що ІБ є невід'ємним елементом загальної проблеми забезпечення інформації особистості, держави і суспільства. Вона зосереджена на захисті важливих або вже згаданих питань джерел інформації, законних інтересів. Зміст поняття «ІБ» розкривається в практичній діяльності, наукових дослідженнях, а також нормативних документах

3. Дослідивши класифікацію засобів інформаційної безпеки було визначено засоби ІБ, які складаються з різноманітних елементів, що охоплюють технологічні, організаційні, правові та фізичні аспекти. Всі вони повинні діяти в комплексі для забезпечення належного рівня захисту від загроз і мінімізації ризиків у різних сферах.

4. В роботі визначені органи державного управління. Основними об’єктами державного управління відповідно до європейського підходу слід вважати підпорядковані органам виконавчої влади, сектори державного управління, промисловість, державні установи, агентства та суб'єкти господарювання, підпорядковані органам виконавчої влади. Отже, об’єкти державного управління - це система, за допомогою якої спрямовується вплив

органів управління. Безпосередніми об'єктами, яких торкається те чи інше конкретне питання, є підгалузі (галузі) державного управління.

5. Проаналізовавши засоби безпеки в органах державного управління, виявили, що одним з основних завдань є отримання та ґрунтовний аналіз інформації щодо захищеності від загроз і умов функціонування об’єктів управління. Це дозволяє своєчасно оцінювати ситуацію, передбачати можливі загрози та коригувати стратегії для їх нейтралізації. Оскільки загрози національній безпеці можуть бути різноманітними та змінюватися в динаміці, ефективне управління безпекою потребує постійного моніторингу і аналізу актуальної інформації.

6. В роботі охарактеризований вплив діяльності органів державного управління на інформаційну безпеку України. Проте, на даний момент в правовій системі України не існує чітких нормативних актів, які б регламентували співробітництво суб'єктів державного управління, уповноважених виконувати функції забезпечення інформаційної безпеки держави.

7. Дослідивши загальну характеристику діяльності ДСЯО можемо зазначити, що одним із ключових завдань служби є організація інституційних аудитів закладів освіти, які спрямовані на оцінку якості управління та освітнього процесу. Під час аудитів враховуються показники результативності навчання, умови для забезпечення якості освіти, педагогічна майстерність викладачів і задоволеність учасників освітнього процесу. Окрім цього, ДСЯО надає консультації та рекомендації для покращення роботи закладів освіти, допомагаючи адаптувати їх до сучасних викликів і стандартів.

8. Під час написання кваліфікаційної роботи ми дійшли до висновку, що вплив засобів ІБ на роботу ДСЯО є суттєвим, адже вона є критично важливою для ефективного функціонування організації, яка оперує значними обсягами чутливих даних про заклади освіти, педагогів та учнів. Надійні засоби ІБ дозволяють зберігати конфіденційність даних, захищаючи їх від

несанкціонованого доступу, що сприяє підтримці довіри до діяльності служби.

9. Також проаналізувавши перспективи впровадження новітніх засобів інформаційної безпеки в роботу ДСЯО ми виявили, що сфера освіти постійно змінюється, і ДСЯО має реагувати на нові виклики, пов’язані з диджиталізацією. Засоби інформаційної безпеки дозволяють розширювати функціонал цифрових інструментів, таких як електронні платформи оцінювання, онлайн-сервіси для навчальних закладів і цифрові документообіги. ДСЯО поступово переходить до електронного документообігу, цифрових платформ оцінювання якості навчання та автоматизованих систем збору даних. Захист цих інноваційних рішень забезпечує ефективність роботи служби, знижує витрати на паперову документацію та пришвидшує обмін інформацією.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Албул С.В. Категорії «розвідувальна інформація» та «інформація розвідки» в оперативно-розшуковій діяльності Національної поліції України». *Економічна та інформаційна безпека: актуальні питання та інновації : матеріали Міжнародної науково-практичної конференції,* м. Дніпро, 04 листопада 2021 р. Дніпро : ДДУВС, 2021. С. 37–38.
2. Албул С.В. Методологія кримінальної розвідки: теоретико-праксеологічний дискурс. *Південноукраїнський правничий часопис*. 2016. № 2. С. 34–37.
3. Албул Г. І., Савчук, Б. П. Інформаційна безпека: навчальний посібник. Київ: НАУ, 2018. С. 45–112.
4. Андрущак Г. І. Інформаційна безпека: теорія і практика. Київ: Знання, 2018. 312 с.
5. Бідюк І. П., Шевченко С. В. Основи інформаційної безпеки: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2017. 284 с.
6. Бойко А. І. Технічні засоби інформаційної безпеки: інтеграція в державних установах. Львів: Світ, 2021. 185 с.
7. Бойко А. І., Сидоренко В. І. Криптографія та захист інформації. Львів: Світ, 2020. С. 78–125.
8. Бойко А. І., Сидоренко В. І. Криптографія та захист інформації. Львів: Світ, 2020. 232 с.
9. Борисов А. А., Коваленко Ю. С. Сучасні технології інформаційної безпеки. Одеса: ОНУ, 2019. С. 45–98.
10. Вишня В.Б., Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки: навчальний посібник. Дніпро: Дніпроп. держ.ун-т внутріш. справ, 2020. 128 с.
11. Герасименко І. А. Комплексна інформаційна безпека освітніх установ. Київ: КНЕУ, 2020. 134 с.

12. Глинський Я. М., Сахно, О. М. Інформаційна безпека: сучасні методи та технології. Київ: Видавничий дім "Кондор", 2019. С. 78–154.
13. Глушков В. М. Методи захисту інформації в інформаційних системах. Харків: Фоліо, 2018. 203 с.
14. Глущенко Ю. В. Інформаційна безпека держави: організаційно-правові аспекти. Київ: Ліра-К, 2017. С. 60–115.
15. Гнатюк С. М., Приймак, А. О. Основи інформаційної безпеки. Київ: НАУ, 2019. С. 90–145.
16. Гребенюк О. А., Писаревський, В. П. Методи та засоби захисту інформації в інформаційно-комунікаційних системах. Київ: НАУ, 2021. С. 45–130.
17. Громовий В. І., Громовий, А. В. Системи захисту інформації.*Харків: ХНЕУ, 2017. С. 22–90.
18. Гур'єв В.І., Мехед Д.Б., Ткач Ю.М., Фірсова І.В. Інформаційна безпека держави: навчальний посібник. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
19. Державна служба спеціального зв'язку та захисту інформації України. Рекомендації щодо забезпечення інформаційної безпеки в органах державної влади. Київ: Держспецзв'язку, 2022.
20. Державна служба якості освіти України. Офіційний вебсайт. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2020/2_2020/36.pdf (дата звернення: 15.11.2024).
21. Закон України "Про захист інформації в інформаційно-комунікаційних системах". Відомості Верховної Ради України. 1994. № 31. URL:https://zakon.rada.gov.ua/laws/show/1222-2020-%D0%BF#Text (дата звернення: 05.12.2024).
22. Закон України "Про інформацію". Відомості Верховної Ради України. 1992. № 48. URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text(дата звернення:17.11.2024).

23. Калюжний М. О. Захист інформації в комп'ютерних системах. Запоріжжя: ЗНТУ, 2018. С. 101–145.
24. Киричок О. О. Захист інформації в освітніх установах: правові та технічні аспекти. Київ: Національна академія внутрішніх справ, 2021. 210 с.
25. Коваленко О. В. Забезпечення інформаційної безпеки в системі освіти: перспективи розвитку. *Збірник наукових праць*. 2022. № 9. С. 88–94.
26. Коваленко О. М. Основи безпеки інформаційних систем. Львів: Львівська політехніка, 2019. С. 54–120.
27. Колесніков О. М., Лещенко, А. А. Організація інформаційної безпеки підприємства. Київ: КНЕУ, 2021. С. 101–178.
28. Кухаренко О. В. Криптографічний захист інформації. Львів: ЛНУ, 2019. С. 65–138.
29. Кушнаренко С. М. Інформаційна безпека в органах освіти: системний підхід. *Збірник наукових праць*. 2021. № 7. С. 45–52.
30. Кушнаренко С. М. Сучасні підходи до забезпечення інформаційної безпеки в органах державного управління. *Збірник наукових праць*. 2020. № 5. С. 22–28.
31. Лапко О. О., Літвінова, Г. О. Кібербезпека: базові концепції та сучасні технології.Київ: Академія, 2020. С. 20–75.
32. Лемешко О. В. Інформаційна безпека: сучасні підходи. Дніпро: ДНУ, 2019. 252 с.
33. Нестеренко М. С. Моделі та методи кібербезпеки. Київ: Кондор, 2020. 198с.
34. Нідзельський М. В., Федорова, О. П. Захист інформації в комп'ютерних системах. Одеса: ОНПУ, 2020. С. 34–98.
35. Павлюк О. П. Правові аспекти забезпечення кібербезпеки. Львів: ЛНУ, 2021. С. 58–123.
36. Паламарчук О. В. Основи криптографії: теорія і практика. Київ: НТУУ "КПІ", 2016. 176 с.

37. Прокопенко М. В. Інформаційна безпека: теоретичні основи і практичні аспекти. Чернігів: ЧНТУ, 2020. С. 77–140.
38. Процик В. І. Інформаційна безпека освітніх даних: національний та міжнародний досвід. *Вісник Київського університету*. 2021. № 5. С. 56–62.
39. Сайко В. А. Кібербезпека та захист інформації. Харків: ХНУРЕ, 2021. С. 101–145.
40. Сікорський В. В. Технології інформаційної безпеки. Київ: Кондор, 2020. С. 80–145.
41. Соколовський І. А. Організація інформаційної безпеки в системі державного управління. Київ: Юрінком Інтер, 2020. 236 с.
42. Сухомлин І. П., Волков, В. П. Захист інформації в інформаційних системах. Харків: ХНУРЕ, 2018. С. 115–180.
43. Тарасенко В. А., Данилюк Ю. А. Інформаційна безпека в комп'ютерних мережах. Київ: Політехніка, 2019. С. 120–180.
44. Шимон С. І., Коваленко О. В. Кібербезпека в державному управлінні: основи захисту інформації. Львів: Видавництво Львівської політехніки, 2021. 186 с.
45. Шимон С. І., Коваленко О. В. Кібербезпека: основи захисту інформації. Львів: Видавництво Львівської політехніки, 2021. С. 156–192.
46. Шокін А. П. Інформаційна безпека в системі державного управління: нормативно-правове регулювання та технічні засоби. Київ: Юрінком Інтер, 2021. 194 с.
47. Щеголєв К. В., Волков, В. П. Основи інформаційної безпеки. Київ: КНЕУ, 2020. С. 50–120.
48. Ярошенко А. В. Системи захисту інформації в інформаційно-комунікаційних мережах. Одеса: ОНАС, 2020. С. 110–165.

ДОДАТКИ

Додаток 1

ЗАТВЕРДЖЕНО
наказ Державної служби
якості освіти України
07.10.2021 № 01-11/72

(в редакції наказу Державної
служби якості освіти України
02.10.2024 № 01-10/259)

ПОЛОЖЕННЯ
про організацію системи безпеки електронної пошти Державної служби якості освіти України

1. Загальні положення

1.1. Це Положення є частиною загальної політики безпеки Державної служби якості освіти України (далі – Служба) в системі безпеки корпоративної мережі та інформації, яке визначає організаційні заходи функціонування засобів мережі Інтернет у Службі. Положення встановлює єдиний порядок надання доступу та використання службових електронних адрес в домені sqe.gov.ua, відправки та отримання електронної пошти і носить обов'язковий характер під час використання службової електронної пошти.

1.2. Основні терміни, що використовуються у цьому Положенні:

1.3. Відповідальна особа за роботу з електронною поштовою скринькою

2. Відповідальна особа за роботу з електронною поштовиою скринькою (далі – відповідальна особа)– працівник Служби, територіального органу Служби та підприємства, установи, організації, що належать до сфери

управління Служби, який в установленому порядку отримав від адміністратора ЕП право доступу до відповідної електронної поштової скриньки з правами та обов'язками щодо відправлення, одержання електронних повідомлень у системі ЕП й дотримання вимог кібербезпеки та кібергігієни.

3. Користувач електронної поштової скриньки (далі – користувач ЕП) - працівник Служби, територіального органу Служби та підприємства, установи, організації, що належать до сфери управління Служби, який в установленому порядку отримав від відповідальної особи право доступу до відповідної електронної поштової скриньки з правами та обов'язками щодо відправлення, одержання електронних повідомлень у системі ЕП й дотримання вимог кібербезпеки та кібергігієни.

Додаток 2

ЗАТВЕРДЖЕНО
наказ Державної служби
якості освіти України
07.10.2021 № 01-11/72

(в редакції наказу Державної
служби якості освіти України
02.10.2024 № 01-10/259)

ПОЛОЖЕННЯ
про порядок надання доступу працівникам Державної служби якості освіти України до використання прикладних програм, баз даних та інформаційних ресурсів

1. Загальні положення

1.1. Це Положення є документом загальної політики безпеки Державної служби якості освіти України (далі – Служба) в частині безпеки доступу до корпоративної мережі та інформації, яке визначає порядок надання, блокування, тимчасового блокування доступу, налаштування прав та повноважень з обробки інформації працівників Державної служби якості освіти України, територіальних органів Служби та підприємств, установ, організацій, що належать до сфери її управління для їх роботи з прикладними програмами, інформаційно-аналітичними, інформаційно (автоматизованими) системами, базами даних, іншими інформаційними ресурсами та комп’ютерної мережі Служби (далі – інформаційні ресурси).

1.2. Основні терміни, що використовуються у цьому Положенні:

Автоматизована система (далі – АС) – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних заходів:

Робоча станція — це засіб комп'ютерної техніки, з яким у певний

проміжок часу може працювати лише один користувач. В інші проміжки часу доступ до тієї ж робочої станції можуть отримувати інші користувачі. Кожен користувач може володіти різними повноваженнями (правами) доступу до інформації, що обробляється на робочій станції.

Комп'ютерна мережа – сукупність робочих станцій, периферійного обладнання, цифрових пристроїв, мережевого та серверного обладнання, яка дозволяє здійснювати доступ до інформації та її обробку різним користувачам із визначеними на це правами доступу.

Адміністратор – уповноважений на роботу в інформаційно-комунікаційній системі (далі – ІКС) працівник Служби якому надано відповідний рівень прав доступу (додаток 1) до функціональних можливостей інформаційного ресурсу, основним завданням якого є встановлення значень параметрів конфігурації ІКС, безпосередньо пов'язаних із доступом до інформації, ведення електронного обліку користувачів, надання їм повноважень в роботі з ІКС та прав доступу до обробки інформації, яка циркулює в ІКС, проведення спостережень за роботою інформаційного ресурсу та аналіз ризиків кіберінцидентів.

Багатофакторна аутентифікація – це використання декількох різних способів підтвердження особи користувача для отримання доступу до інформаційного ресурсу, де першим фактором є пароль, іншими факторами можуть виступати: код підтвердження, смс повідомлення, дзвінок за номером телефона, лист на резервну електронну пошту тощо.

Користувач – працівник Служби, територіального органу Служби або підприємства, установи, організації, що належать до сфери управління Служби, який згідно з установленим порядком отримав право доступу до обробки інформації в інформаційних ресурсах Служби.

Користувач ЦА – користувач з числа працівників центрального апарату Служби, який отримав доступ до інформаційних ресурсів та обладнання Служби, у тому числі робочої станції з попередньо встановленим

програмним забезпеченням, визначеним в описі програмного забезпечення типового робочого місця користувача.

Користувач ТО - користувач з числа працівників територіального органу, підприємства, установи, організації, що належать до сфери управління Служби, який отримав доступ до інформаційних ресурсів Служби.

Логін – послідовність символів, що ідентифікує кожного окремого користувача серед інших користувачів інформаційного ресурсу (номер телефону, адреса електронної пошти, або набір символів).

Облікові дані – дані користувача, які використовуються для його ідентифікації (логін і пароль) та надання авторизованого доступу до інформаційного ресурсу.

Обробка інформації – виконання операцій, зокрема: збирання, введення, записування, перетворення, зберігання, роздрукування, знищення, приймання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Пароль – послідовність символів, що відома лише певному користувачу, зберігається в інформаційному ресурсі у зашифрованому вигляді і використовується виключно для авторизованого доступу користувача до нього.

Підпорядковані установи – територіальні органи Служби, підприємства, установи і організації, що належать до сфери управління Служби.

1.3. Будь-який доступ, у тому числі тимчасовий, до інформаційних ресурсів та комп’ютерної мережі Служби, крім випадків передбачених цим Положенням, заборонений.

1.4. Надання, блокування, тимчасове блокування прав та повноважень користувача з обробки інформації в інформаційних ресурсах Служби, описаних в розділах 2 (для центрального апарату Служби) та 3 (для підпорядкованих установ), надається **виключно** за погодженням керівництва

Служби, крім випадків визначених пунктами 1.5, 1.6 та 1.14 цього Положення.

1.5. Адміністратор може надати доступ до інформаційного ресурсу представнику надавача послуг з технічної підтримки з метою виконання робіт з налаштувань, визначеним представникам основних суб'єктів національної системи кібербезпеки, адміністратору вищого рівня або для навчання нового адміністратора. Усі роботи з налаштувань та перевірок інформаційних ресурсів відбуваються під наглядом адміністратора або представника підрозділу адміністратора.

1.6. Особам, які не є працівниками Служби та проходять практику, стажування, навчання, приймають участь в заходах Служби за дозволом керівництва Служби (доповідна записка про надання доступу (додаток 2) та згода на оброку персональних даних особи (додаток 4)) може бути надано тимчасовий доступ до комп'ютерної мережі, робочої станції та інформаційного ресурсу з дотриманням внутрішніх політик безпеки.

У приміщеннях, призначених для прийому громадян, забезпечується доступ через локальну мережу до ресурсів, в обсязі, що визначений нормативно-правовими актами.

Додаток 3

Базові рекомендації щодо обмеження використання Telegram в організації

Організаційні заходи

1. Розробити та затвердити внутрішнім документом (наказ, розпорядження тощо) політику використання Telegram в організації, якою передбачити:
   - заборону передання інформації, яка використовується в роботі, а також здійснення комунікацій зі службовою метою з використанням месенджера Telegram;
   - заборону встановлення і використання клієнта Telegram та/або використання вебверсії Telegram на службових комп'ютерах та особистих комп'ютерах, що використовуються в службовій діяльності організації;
   - визначення переліку осіб організації, яким згідно з посадовими обов'язками належить використання Telegram у службовій діяльності;
   - порядок формування та ведення переліку осіб організації, яким згідно з посадовими обов'язками належить використання Telegram;
   - порядок роботи з наявними службовими обліковими записами Telegram (каналами, ботами тощо), основні заходи безпеки під час роботи з ними;
   - впровадження в організації технічних заходів обмеження доступу до Telegram з урахуванням наявної інфраструктури доступу в інтернет та засобів кібербезпеки;
   - визначення підрозділу (посадових осіб), відповідальних за контроль.
2. Довести до працівників розроблену політику, а також поінформувати їх про причини блокування Telegram в організації та потенційні ризики для безпеки, пов'язані з його використанням.

Технічні заходи

В залежності від наявних засобів кібербезпеки:

- забезпечити фільтрацію трафіку Telegram на рівні файрвола (NGFW), системи виявлення втручань (IPS), проксі-сервера. Для цього налаштувати правила для фільтрації (блокування) трафіку на сервери Telegram та з них, у випадку відсутності технічних можливостей – створити правила, що забороняють зв'язок з доменами, які використовує Telegram;
- створити окремий мережевий сегмент (VLAN) для пристроїв, із яких здійснюється санкціонований доступ до Telegram;
- якщо в організації передбачено використання бездротових (WiFi) мереж, створити відповідні правила для бездротового сегмента;
- забезпечити фільтрацію Telegram через налаштування системи доменних імен DNS. Запобігаючи отриманню відповіді про доменні імена, пов'язані з Telegram, користувачі не зможуть підключитися до сервісу. Наявна можливість підключення до Національного сервісу DNS у тестовому режимі, що забезпечить також додатковий захист від кібератак;
- налаштувати рішення для захисту кінцевих точок (антивірус, EDR тощо), які мають функції контролю додатків, на блокування Telegram;
- налаштувати групові політики в середовищі Windows, щоб обмежити можливість користувачів встановлювати та виконувати Telegram на службових комп’ютерах;
- налаштувати механізми моніторингу та реєстрації подій безпеки, для виявлення спроб доступу до Telegram;
- періодично оновлювати технічні заходи блокування, щоб врахувати зміни в інфраструктурі Telegram.