МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

МАЗУРКЕВИЧ ТАЇСІЯ ЛЕОНІДІВНА

Допускається до захисту:
завідувач кафедри інформаційних систем управління
д-р екон. наук, професор
_____ О.М. Анісімова
«____»_____ 20___ р.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА ДІЯЛЬНІСТЬ І БЕЗПЕКА В СУСПІЛЬСТВІ

Спеціальність 029 Інформаційна, бібліотечна та архівна справа

Кваліфікаційна (бакалаврська) робота

Керівник:
Ковальська Л.А., професор кафедри
інформаційних систем управління
д-р істор. наук, доцент

Оцінка: ____ / ___ / _____
(бали / за шкалою ЄКТS / за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця – 2021

АНОТАЦІЯ

Мазуркевич Т.Л. Інформаційно-комунікаційна діяльність і безпека в суспільстві. Спеціальність 029 «Інформаційна, бібліотечна та архівна справа» Донецький національний університет імені Василя Стуса, 2021.

Розкрито теоретичні основи реалізації та особливості інформаційно-комунікаційної діяльності і безпеки в суспільстві. Досліджено особливості функціонування інформаційно-комунікаційної безпеки в суспільстві, розглянуто систему захисту інформації та комунікації з врахуванням потреби захисту інформації та комунікації. Проаналізовано автоматизовані системи захисту інформації та комунікації. Встановлено необхідність впровадження і регулярного оновлення систем захисту інформації в роботі органу влади.

Ключові слова: інформаційно-комунікаційна діяльність, інформаційна безпека, суспільство, захист інформації, інформаційна загроза.

Табл. 11. Рис. 17. Бібліограф.: 67 найменування.

Mazurkevych T.L. Information and communication activities and security in society. Specialty 029 Information, library and archival affairs. Vasyl Stus Donetsk National University, 2021.

Theoretical bases of realization and features of information and communication activity and safety in a society are opened. The peculiarities of the functioning of information and communication security in the society are studied, the system of information protection and communication is considered, taking into account the need for information protection and communication. Automated information protection and communication systems are analyzed. The need for introduction and regular updating of information protection systems in the work of the authority has been established.

Key words: information and communication activity, information security, society, information protection, information threat.

Table. 11. Fig. 17. Bibliographer: 67 items.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Особливості інформаційно-технологічного розвитку XXI століття визначають використання і вдосконалення інформаційних технологій та технічних засобів комунікації. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах в роботі органів влади гарантується нормативними актами та становить важливий напрям роботи з інформацією. Достатність впроваджених засобів захисту інформації обґрунтовується на етапі технічного проектування системи захисту інформації та оцінюється під час проведення державної експертизи комплексної системи захисту інформації. Відповідальність за забезпечення захисту інформації в системі інформаційно-комунікаційної діяльності органів влади покладається на власника системи.

Крім того, захисту інформації потребує повсякденне життя сучасної людини, яка використовує різну інформацію і зберігає її на різноманітних технічних пристроях. Одним з найпоширеніших, щоденним супутником кожної людини є смартфон, який з простого засобу зв’язку перетворився на засіб комунікації, носій особистісної інформації, механізм реалізації потреб та можливості виконувати роботу, навчання, різні питання життя (банківські операції, медицина, публічне життя, посвідчення особи та інші). Зрозуміло, що з розширенням можливостей інформаційно-комунікаційної діяльності і використання смарт-пристроїв, зростає і небезпека витоку та втрати даних.

Тому, інформаційна безпека сьогодні стала неодмінною умовою життя і діяльності державних органів, підприємств і усіх користувачів. Можливості убезпечення інформації в сучасному віртуальному просторі постійно вдосконалюються, а всім учасникам цього віртуального життя варто подбати про належний рівень безпеки (кібербезпеки) як цифрових пристроїв так і власної інформації.

Мета дослідження: розкрити особливості інформаційно-комунікаційної діяльності в суспільстві та виявити тенденції розвитку систем захисту інформації та комунікації.

Реалізація мети передбачає послідовне вирішення наступних **завдань:**

- вивчити особливості інформаційно-комунікаційної діяльності і безпеки інформації;

- подати характеристику інформаційно-комунікаційної діяльності в суспільстві;

- дослідити розвиток систем захисту інформації та технологічної безпеки комунікації;

- проаналізувати потреби та можливості захисту інформації та комунікації;

- опрацювати можливості автоматизованих систем захисту інформації та комунікації;

- обґрунтувати необхідність захисту інформації органів влади та персональних даних;

- розглянути можливості використання технічних і технологічних засобів захисту у роботі з інформацією;

- конкретизувати потребу впровадження систем захисту інформації на прикладі органу державної влади та усіх користувачів і учасників інформаційно-комунікаційного простору.

Об’єктом дослідження є інформаційно-комунікаційна діяльність та захист інформації.

Предмет дослідження є сучасні можливості інформаційно-комунікаційної діяльності, в якій виникає небезпека цілісності та збереження інформації і актуалізується необхідність впровадження систем захисту інформації.

Практичну значимість роботи визначає аналіз сучасних технологічних можливостей інформаційно-комунікаційної діяльності, особливості роботи у віртуальному просторі, небезпека та загроза інформації і необхідність її захисту від нецільового використання та злочинних дій в умовах розвитку інформаційного суспільства.

Апробація результатів дослідження. Окремі аспекти бакалаврської роботи були представлені у науковій статті Віснику студентського наукового товариства Донецького національного університету імені Василя Стуса (м. Вінниця, 2019); обговорені на конференціях та опубліковані у збірниках матеріалів IV, V, та VI Всеукраїнської наукової студентської конференції «Інформаційні технології і системи в документознавчій сфері» (м. Вінниця, 2019, 2020, 2021).

Структура кваліфікаційної (бакалаврської) роботи визначена метою і завданнями та складається із вступу, трьох розділів восьми підрозділів, висновків, списку використаних посилань, додатків. Список використаних посилань включає 67 найменувань. Робота викладена на 62 сторінках друкованого тексту, основна частина якої становить 52 сторінки. Додатки представляють два ілюстративні інформаційні документи.

РОЗДІЛ 1
ОСОБЛИВОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ ДІЯЛЬНОСТІ І БЕЗПЕКИ ІНФОРМАЦІЇ

1.1. Основний зміст інформаційно-комунікаційної діяльності в суспільстві

Становлення і розвиток інформаційного суспільства, яке спостерігається в сучасних умовах, є відмінною рисою XXI століття. В інформаційному суспільстві активно розвиваються інформаційні і комунікаційні технології, створюються умови для ефективного використання знань у вирішенні найважливіших завдань управління суспільством і демократизації суспільного життя. Ці процеси сприяють формуванню інформаційного простору, в якому створюється, транслюється, реалізується і накопичується інформація. Інформаційний простір – це історично сформована, забезпечена правовими гарантіями й засобами зв'язку, з найбільшою доступністю для споживача, форма скоординованих і структурованих, територіально близьких і віддалених інформаційних ресурсів, котрі акумулюють результати комунікаційної діяльності людей.

Знання та інформація породжують нові знання, їх обсяги і вплив на продуктивний розвиток суспільства зростає у геометричній прогресії.

Змістове наповнення інформаційного суспільства можна подати у вигляді наступних характеристик:

- будь-хто, будь-де й у будь-який час може одержати за відповідну плату чи безкоштовно на основі автоматизованого доступу і систем зв'язку будь-яку інформацію і знання, необхідні для їхньої життєдіяльності та вирішення особистих і соціально значущих завдань;
- у суспільстві виробляється, функціонує і доступна будь-якому індивіду, групі чи організації сучасна інформаційна технологія;

- існують розвинені інфраструктури, що забезпечують створення національних інформаційних ресурсів у обсязі, необхідному для підтримки науково-технологічного і соціально-історичного прогресу;
- відбувається процес прискореної автоматизації і роботизації всіх сфер і галузей виробництва та керування;
- здійснюються радикальні зміни соціальних структур, наслідком яких є розширення сфери інформаційної діяльності та послуг.

З-поміж згаданих ознак пріоритетне місце посідає комунікаційна діяльність з використанням сучасних технологій і технічних засобів. Інформаційно-комунікаційна діяльність, явище не нове в існуванні суспільства, але сьогодні воно отримало інше змістове наповнення і стало необхідною умовою життя і розвитку суспільства. Тут можна запропонувати наступне визначення цього поняття, яке включає в себе всю суть і структуру такого неодмінного атрибуту сучасної людини.

Інформаційно-комунікаційна діяльність (ІКД) – це система обміну інформацією між та населенням, організаціями різних форм власності за допомогою спеціальної системи символів, кодів, засобів та організаційних форм; соціальна взаємодія, що має низку специфічних властивостей і ознак, спрямована на регулювання поведінки людей, роботи інститутів державної влади заради досягнення певної мети [12, с.163].

У сучасному суспільстві у зв’язку зі зростанням ролі інформаційно-комунікаційних технологій зростає потреба захисту даних від втрати, викрадення, спотворення або пошкодження. А це в свою чергу потребує посиленої безпеки інформаційної діяльності в суспільстві. Вирішення цієї проблеми сприяє забезпеченню інформаційної безпеки як окремої особистості, організації, так і всієї держави. Інформаційна безпека – стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз.

Розроблені Закони та нормативні акти України гарантують умови розвитку інформаційного суспільства, регулюють безпеку інформації, визначають межі

встановлення, розвитку та регулювання інформаційних відносин (Про інформацію, Про доступ до публічної інформації тощо). Положення Законів України та інших нормативно-правових актів, які мають безпосереднє відношення до інформаційних відносин, мають спрямованість саме на захист інформації. Положення зі спрямованістю на захист людини, суспільства, а й відповідно, держави від інформації знаходяться у «меншості».

Стрижнем розуміння сутності поняття «інформаційна безпека» є розуміння сутності поняття «інформація» [24, с.80]. Відомо, що отримання інформації здійснюється через всі чотири органи, якими людину наділила природа: зір, слух, відчуття та дотик [18, с. 167]. Можливості вироблення та транслювання інформації і її подальше зберігання органами чуттів людини одночасно є й слабким її місцем. Виникає потреба убезпечити інформацію, проконтролювати її використання і гарантувати її цілісність, адекватність, достовірність. Якщо навести приклади, то інформаційна безпека – це про захист коштів на банківській картці, цілісність медичних даних у системі helsi, не заборонений контент у соціальних мережах, неможливість стороннього редагування законів на rada.gov.ua, конфіденційність повідомлень у месенджерах, а також захист від кібератак об’єктів критичної інфраструктури.

Важливість інформаційної безпеки та зберігання важливих даних, при якому забезпечено конфіденційність, доступність і цілісність даних є стан захищеності систем передавання [9, с. 261].

Розглянемо види загроз інформаційній безпеці, що стають можливими за рахунок недосконалої системи захисту даних під час інформаційної комунікації:

- отримання доступу до секретних або конфіденційних даних;
- порушення або повне припинення роботи комп’ютерної інформаційної системи;
- отримання доступу до керування роботою комп’ютерної інформаційної системи;
- знищення або спотворення даних.

Інформаційна безпека також включає в себе комплекс заходів, які повинні забезпечити захищеність даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення. Поняття інформаційно-комунікаційна діяльність представлено у таблиці 1.1. [36, с.105].

Таблиця 1.1. – Поняття інформаційно-комунікаційна діяльність

Автор	*Визначення*
Крупінський С.Н.	атрибут діяльності органів влади в сучасних умовах, виконуючи цілу низку важливих функцій. На сучасному етапі розвитку українського суспільства особливого значення набуває їх використання під час побудови взаємодії з інститутами громадянського суспільства
Лихачев М.Г.	інформація на основі підходів «нової публічної служби» сьогодення сприятимуть зміцненню авторитету органів влади, зростанню громадської активності, підвищенню обґрунтованості управлінських рішень
Шаповал Ю.Я.	інструмент розкриття потенціалу громадських структур, забезпечення більш активної участі громадян у діяльності органів державного управління, а також підвищення відповідальності та підзвітності влади, побудові сучасної демократичної системи державного управління.

Єдиного визначення цього поняття не існує, кожен автор вкладає у це вагому складову, яка відображає спрямованість діяльності, учасників, інформаційне повідомлення, канал зв’язку тощо. Останнім часом до питань інформаційної безпеки включено питання інформаційного впливу на особистість і суспільство.

У зв’язку зі зростаючою роллю інформаційно-комунікаційних технологій у сучасному суспільстві проблема захисту даних може бути виражена у наступних видах:

1) втрата;

2) викрадення;

3) спотворення;

4) пошкодження [27, с.135].

«Інформаційна безпека» має суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи, а також суспільства і держави за безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані з організацією технологій створення, розповсюдження, зберігання та використання інформації (відомостей, службових даних чи інших знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави [13, с.120].

Інформаційна безпека посідає одне з ключових місць у системі забезпечення життєво важливих інтересів усіх без винятку країн. Це в першу чергу обумовлено нагальною потребою створення розвиненого інформаційного середовища суспільства [39, с.153].

У лютому 2017 року указом Президента України було затверджено Доктрину інформаційної безпеки України, яка визначила національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [7]. Життєво важливими інтересами суспільства та держави визнано такі:

• захист українського суспільства від агресивного впливу деструктивної пропаганди;

• захист українського суспільства від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної та релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

• усебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірних та об'єктивних відомостей та інші [28, с.106].

У сучасних умовах техніко-технологічного розвитку суспільства виникла потреба в переосмисленні та уточненні проблеми інформатизації України крізь призму її інформаційної безпеки з урахуванням сучасних інформаційних

впливів. Розглянемо визначення специфіки інформаційної безпеки різних авторів з різних точок зору та підходів дослідження безпеки інформації наведене у таблиці 1.2.

Таблиця 1.2. — Дефініції «інформаційна безпека»

Автор	*Визначення*
Хоффман Л.Дж.	це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації
Литвиненко О.	одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами
Горбатюк О.	стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
Богуш В.	стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави
Сороківська О.	суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб’єкта господарської діяльності
Бурячок В.	стан захищеності кіберпростору держави загалом або окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам

Призначення соціальної комунікації полягає у виконанні комунікативної функції соціуму, а також можливості їх приєднання через засоби комунікування до інформаційних агентств і міжнародних організацій [28, с.106]. Теперішня

комунікація представляє соціальне явище яке є засобом забезпечення взаємозв'язку людей у їх діяльності.

Сьогодні не зовсім точним є уявлення, наскільки серйозною інформаційна безпека є в умовах сучасної геополітичної обстановки України і як обернеться для населення найближчим часом маніпулювання сенсом (змістом) інформаційних повідомлень. Глобалізація способу життя і джерел постачання інформації багато в чому вже дискредитували їх дії при визначенні національних інтересів і цінностей та зруйнували соціокультурну ідентичність громадян [46, с.191].

У цьому аспекті, головною метою інформаційної-комунікативної діяльності є виключення будь-якої можливості зловживань при визначенні прав і свобод людини в інформаційній сфері [45, с. 196].

Сьогодні інформаційна безпека посідає одне з ключових місць у системі забезпечення життєво важливих інтересів усіх без винятку країн. Ознаки інформаційної і комунікаційної безпеки відображено на рисунку 1.1 [33, с.194].

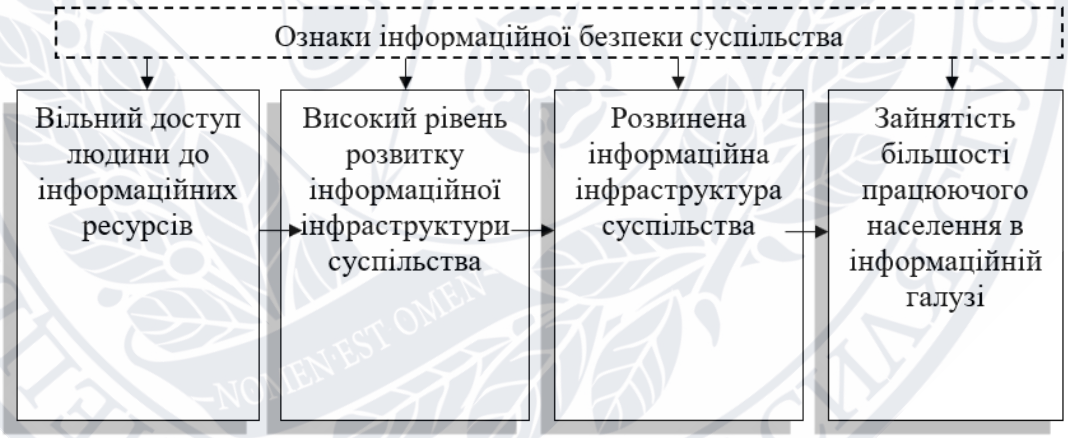

Рисунок. 1.1. — Ознаки інформаційної безпеки суспільства

Інформаційна безпека вимагає забезпечення обмеженого доступу до даних на основі розподілу прав доступу, захисту від несанкціонованого ознайомлення та вивчення їх принципів [31, с.90]. Серед основних виділяємо принцип цілісності даних, конфіденційність, достовірність доступність.

Розглянемо принципи інформаційної безпеки (рисунок 1.2) [25, с.193].

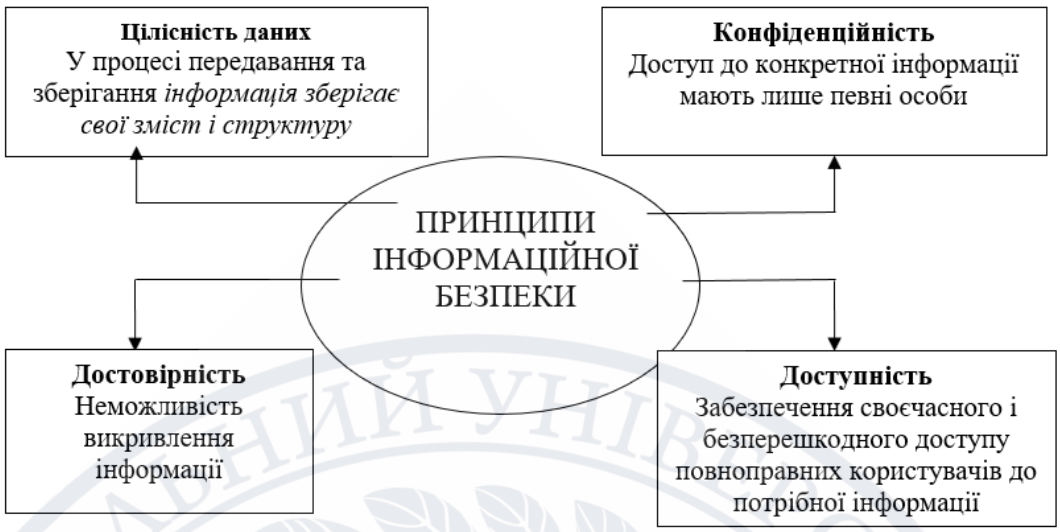

Рисунок. 1.2. – Принципи інформаційної безпеки

Інформаційна безпека також включає в себе комплекс заходів, які повинні забезпечити захищеність даних від несанкціонованого доступу, використання, оприлюднення, внесення змін, знищення [29, с.186]. У сучасному світі, повному протиріч, конфліктів, обтяженому глобальними проблемами, насиченому зброєю, розділеному військовими інтересами і блоками, з реаліями інформаційних загроз та інформаційної війни всередині країни і між державами не уникнути.

У зв'язку зі зростанням ролі інформаційно-комунікаційних технологій у суспільстві зростає проблема захисту даних від втрати, викрадення, спотворення або пошкодження. Вирішення цієї проблеми сприятиме забезпеченню інформаційної безпеки як окремої особистості, організації, так і всієї держави.

1.2. Загальна характеристика інформаційно-комунікаційної безпеки в суспільстві

Інформаційно-комунікаційна діяльність та безпека інформації безумовно пов'язані між собою. Оскільки зміст поняття «безпека» визначається вибором об'єкта захисту. І якщо цим об'єктом виступає власне інформація, тоді поняття як «інформаційна безпека» та «безпека інформації» синонімічна.

Для сучасного етапу розвитку світової цивілізації характерний перехід від індустріального суспільства до інформаційного, формування якого пов'язують із розвитком інформаційних технологій, що радикально змінюють суспільне життя. Є різноманітні підходи тлумачення процесів становлення й розвитку інформаційного суспільства, навіть у розвинених країнах світу. В суспільстві присутній комплекс організаційних, технічних і програмних засобів, методів і заходів до комп'ютерної інформації. Розглянемо у схематичному вигляді загрози інформаційній безпеці відображені на рисунку 1.3 [37].

Рисунок 1.3. – Загрози інформаційній безпеці

Технології володіння й обміну змістовною інформацією як ресурсом розвитку завжди визначали основні вимоги до якості інформаційно-комунікаційного простору будь-якої країни. З появою комп'ютера із низкою новітніх інформаційно-комунікаційних технологій утворилося безліч незнаних досі проблем їх безпеки. Також виявилося багато прорахунків в організації та їх виконанні в процесі інформаційної діяльності [15, с. 134].

У різних формах виникала потреба обміну досвідом та запозичення напрацювань. Особливо при створенні власних баз даних комп'ютерної інформації, різноманітних віртуальних інформаційних продуктів, витісняючи чужі на периферію й захищаючи власні інтереси в інформаційно-

комунікаційній сфері. Особливо це питання актуальне щодо впровадження сучасних і перспективних ІКТ в економічній, військовій, науково-освітній діяльності держави [29, с. 186].

На сьогодні інформаційна безпека має два принципово різні прояви:

1) інформаційно-технічні (прикладом яких є кібератаки);

2) інформаційно-гуманітарні (прикладом яких є операції впливу).

Спрямованість цих двох моделей підпорядкована завданням управління свідомістю людини й відрізняється лише засобами. Рівень освіти й технічні уявлення про складні процеси комп'ютерної доби почали диктувати нові базові принципи захисту джерел інформації від витоку технічними каналами, почали з'являтися ідеї обґрунтувати право на збройну відповідь на кібератаки.

Взагалі терміни «інформаційна війна» і «інформаційна зброя» стали доволі вживаними для пояснення різноманітних дій і операцій інформаційного впливу проти України, які спрямовані на враження індивідуальної й масової свідомості і є зазіханнями на право володіння інформаційними ресурсами [41, с.219].

Основним завданням фахівців у сфері захисту комп'ютерної інформації є убезпечення її від несанкціонованого доступу, модифікації або знищення. В інформаційних системах сьогодні сконцентрована величезна кількість відомостей про різні сфери діяльності. Інформаційні системи мають захист комп'ютерної інформації, яка зберігається в них [24, с. 60].

Захист інформації можна побачити:

1) широкому сенсі – захист інформації як відомостей незалежно від форми їх подання;

2) вузькому сенсі – в інформаційних системах – комп'ютерної інформації.

На сьогодні небезпека несанкціонованого доступу полягає в тому, що створені передумови для здійснення більш тяжких правопорушень – розкрадання комп'ютерної інформації, шпигунства тощо. Основні симптоми присутності вірусів в системі наведено у таблиці 1.3.

Таблиця 1.3. – Основні симптоми присутності вірусів в системі

1	в папці WINDOWS \ SYSTEM32 \ файл MSBLAST.EXE, TEEKIDS.EXE або PENIS32.EXE;
2	у списку запущених процесів є один із вище вказаних файлів;
3	через кілька хвилин роботи в Інтернеті відбувається перезавантаження комп'ютера;
4	у роботі програми MS-Office спостерігаються багатократні сполучення;
5	з'являються повідомлення про помилки, пов'язані з файлом SVCHOST.EXE;
6	на екрані з'являється вікно з повідомленням про помилку RPC Service

Комп'ютерну інформацію можна умовно розподіляти:

1) на машинному носії – лазерні диски та інші носії інформації, які дозволяють відтворювати, редагувати, обробляти, декомпілювати, поширювати наявну на них інформацію виключно за допомогою ПК;

2) на жорсткому диску ПК, наприклад, у вигляді програм (для подання даних із метою отримання певного результату) чи їх модифікації;

3) в системі ПК або їх мережі, здатній обробляти цю інформацію одночасно або здійснювати з нею будь-які маніпуляції (адаптація, модифікація, відтворення, поширення тощо) [49, с.85].

Захист інформації в широкому сенсі розглядається як комплекс питань, пов'язаних із забезпеченням інформаційної безпеки. Загальну характеристику інформаційно-комунікаційної безпеки в суспільстві представлено у таблиці 1.4.

Таблиця 1.4. – Інформаційно-комунікаційна безпека в суспільстві

№	Захист інформації	Уразливості комп'ютерної інформації
1.	Форми їх подання	Схильність до її фізичного знищення
2.	Інформаційні системи	Можливість несанкціонованого доступу (навмисне або з необережності)
3.	Модифікування, копіювання	Небезпека несанкціонованого (умисного чи з необережності) втручання

Об’єктивна необхідність захисту комп’ютерної інформації в сучасних інформаційних системах обумовлена низкою факторів, пов’язаних із побудовою систем захисту країни в умовах ведення проти неї інформаційної війни.

Основними факторами, які сприяють підвищенню уразливості комп’ютерної інформації є:

- різке збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою комп’ютерів;
- зосередження в єдиних базах даних інформації різного призначення і різної приналежності;
- значне розширення кола користувачів, які мають безпосередній доступ до інформаційних ресурсів в системах і мережах [38, с.247].

Електронною версією певної інформації можуть бути: архіви, наукові статті, публіцистичні матеріали ЗМІ, інтерв’ю, звернення, фото, відео, окремі сайти та блоги тощо.

Систематизований перелік шляхів несанкціонованого доступу до інформації в електронному вигляді вбачається так: зчитування даних в масивах інших користувачів; читання залишкової інформації після виконання санкціонованих запитів; маскування під зареєстрованого користувача за допомогою викрадання паролів і інших реквізитів розмежування доступу; маскування несанкціонованих запитів під запити операційної системи (містифікація); використання програмних пасток, а також навмисне виведення з ладу механізмів захисту [45, с.163-164].

У зв’язку з цим значення набуває питання захисту інформації в персональних комп’ютерах, які широко увійшли в нашу повсякденну діяльність [41, с.199]. Звідси виникають, щонайменше, два завдання захисту комп’ютерної інформації: 1) захист комп’ютерної інформації, що знаходиться в персональних комп’ютерах, від несанкціонованого доступу з боку інших осіб за допомогою комп’ютера або з боку мережі; 2) захист інших комп’ютерів та їх мереж від

несанкціонованого доступу з використанням одного з персональних комп'ютерів даної мережі.

Підвищеної актуальності набуває також проблема захисту комп'ютерної інформації в інформаційних мережах, що обумовлено, з одного боку, широким розповсюдженням мереж різного рівня і призначення – від локальної до глобальної, а з іншого – незахищеністю інформації в лініях зв'язку, особливо якщо вони проходять по території, де контроль утруднений. Адже для доступу до комп'ютерної інформації в даному випадку достатньо буде підключитися до цієї лінії або перехопити її в разі передачі комп'ютерної інформації по бездротових каналах зв'язку [41, с.129].

На сьогодні уніфікований підхід до класифікації загроз інформаційній безпеці відсутній (таблиця 1.5). Це виправдано при всьому різноманітті інформаційних систем, спрямованих на автоматизацію технологічних процесів.

Таблиця 1.5. – Узагальнені моделі інформаційних загроз

№	Джерела / канали реалізації загроз	Характеристика прояву загроз	Заходи захисту від загроз
1.	Інформаційні технології	Занепад власних технологій обробки інформації. Імпортування запозичених інформаційних технологій	Розробка власної інформаційної технології Розробка методів стиснення інформації
2.	Інформаційні ресурси	Перевантаження інформацією Перевантаження інформацією Приховування інформації	Оцінка інформації на повноту Розробка методів виявлення дезінформації
3.	Свідомість людини	Суб'єктивність оцінки інформації	Автоматизація ІАД

Отже, сучасна корпоративна система інформаційної безпеки покликана забезпечувати захист конфіденційної інформації від несанкціонованого доступу, запобігати зловмисним або випадковим змінам і давати необхідний рівень доступу. Сьогодні коли питання інформаційно-комунікаційної діяльності в суспільстві набувають глобального характеру, інформаційна безпека є невід'ємною складовою системи безпеки й держави загалом.

РОЗДІЛ 2
РОЗВИТОК СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ТА ТЕХНОЛОГІЧНОЇ БЕЗПЕКИ КОМУНІКАЦІЇ

2.1. Потреби захисту інформації та комунікації

Процес життєдіяльності потребує використання різних комунікацій. Майже неможливо переоцінити важливість комунікацій в управлінні. Практично все, що роблять керівники, аби полегшити досягнення цілей організації, потребує ефективного обміну інформацією. Якщо люди не зможуть обмінюватися інформацією, то вони не зможуть і працювати разом, формулювати цілі й досягати їх, розвиватися та вдосконалюватися [49, с. 115].

Інформаційно-комунікаційні технології (далі - ІКТ) в умовах сучасного динамічного розвитку глобальної інформаційної інфраструктури відіграють ключову роль у зростанні соціально-економічного та бізнес-середовища будь-якої країни, позитивно впливають на швидке налагодження зв’язків у сферах торгівлі, фінансів, транспортування, сприяють активному співробітництву країн з впливовими міжнародними організаціями [28, с. 90].

Завдяки впровадженню останніх досягнень ІКТ у бізнес-середовище відбувається збільшення продуктивності праці робітників, перш за все завдяки підвищенню мобільності та дистанційному доступу до продуктивних систем (ERP), прискорюються та спрощуються внутрішні та зовнішні комунікації.

Саме розвиток ІКТ сприяв виникненню такого нового сегменту в сфері торгівлі, як електронна комерція, що наразі стрімко зростає та сприяє створенню новітніх торговельних онлайн-майданчиків для спрощення пошуку контрагентів та швидкого взаємозв’язку із ними.

Комунікація є складним процесом, який реалізується із взаємозалежних кроків. Кожен з цих кроків потрібен для того, щоб зробити наші думки зрозумілими, кращими. Кожен крок являється, зрозумілим, продуманим, кращим, змістовним і неповторним [49, с. 107]. Комунікації є процесом

передавання інформації від однієї особи до іншої. Для ефективної комунікації вважливий процес передавання повідомлення, коли отримане повідомлення якомога близьке за значенням до первинного. У таблиці 2.1.наведено динаміку IDI України за останні роки. Індекс розвитку ІКТ (IDI: ICT Development Index) використовують для моніторингу та порівняння розвитку інформаційно-комунікаційних технологій.

Таблиця 2.1. – Динаміка IDI України, 2017-2020 рр.

Рік	2017 р.	2018 р.	2019 р.	2020 р.
Рейтинг у світі	60	63	74	62
Показник IDI	3,91	4,98	4,63	5,3

Дані, наведені у таблиці 2.1 свідчать про втрату Україною позицій як технологічно орієнтованої країни та її все більшу інформаційну вразливість, а отже й залежність від світових країн-лідерів у сфері ІКТ. Показник IDI вказує на виробництво країною продукції з високою часткою доданої вартості, про рівень інноваційної компоненти в структурі галузей країни. На жаль, показник IDI України за дослідний період демонструє технологічну відсталість вітчизняної економіки [32, с. 109].

Не впровадження сучасних інноваційних процесів та високотехнологічних складових, що базуються на ІКТ, перешкоджає автоматизації виробництва, уповільнює виробничий процес, призводить до неефективного використання ресурсів та часу, а відтак, й до подорожчання отриманої продукції та її не конкурентоспроможності на світовому ринку, що негативно відображається у структурі платіжного балансу України.

Разом з тим, продаж НКРЗІ 3G ліцензії у лютому 2019 року провідним операторам мобільного зв’язку України вказує на прорив у вітчизняній телекомунікаційній сфері за останнє п’ятиріччя. Незважаючи на те, що із впровадженням цього стандарту зв’язку у повсякденну роботу мобільних пристроїв швидкість доступу до мобільного Інтренету всього 1-2 Мбіт/с, (із позначкою в 30-40 Мбіт/с роботи 3G - мережі в лабораторних умовах), можна

констатувати сплеск у використанні трафіку за допомогою саме мобільних пристроїв. В свою чергу це зумовило збільшення обміну інформацією між користувачами, пришвидшення робочих процесів в бізнес-середовищі, динамічний перехід провідних послуг державного сегменту у Інтернет-простір. Ці тенденції використання та сприяння розвитку ІКТ простежуються у таблиці 2.2 [33, с.231].

Таблиця 2.2 – Використання інформаційно-комунікаційних технологій

№	Можливості / перспективи	Наслідки
1.	використовувати у навчанні здобутки новітніх інформаційних технологій	забезпеченню реалізації інтерактивного підходу (постійне спілкування з ПК, постановка запитань, які цікавлять учня та отримання відповідей на них)
2.	удосконалювати навички самостійної роботи учнів в інформаційних технологіях	підвищує пізнавальну активність учнів за рахунок різноманітної відео та аудіо інформації

Все це дозволить економити час, оптимізувати витрати, ефективно використовувати ресурси як в бізнесі, так і в уряді. Звичайно, на міжнародній арені рейтинг України (як технологічної країни) підвищиться, що призведе до залучення додаткових коштів у сферу ІКТ України. За таких умов, та із налагодженням політичної ситуації на сході України, можна очікувати зниження витрат державного бюджету України та збільшення його надходжень. Розвиток ІКТ в Україні сприятиме залученню додаткових коштів, збільшенню робочих місць, відкриттю нових сегментів в бізнес-середовищі, зростанню рівня освіченості населення, а отже й росту людського капіталу. Безумовно, все це позитивно впливатиме на зростання добробуту української нації. Окремо унаочнено динаміку розвитку і реалізації інформаційно-комунікаційних технологій (рисунок 2.1.).

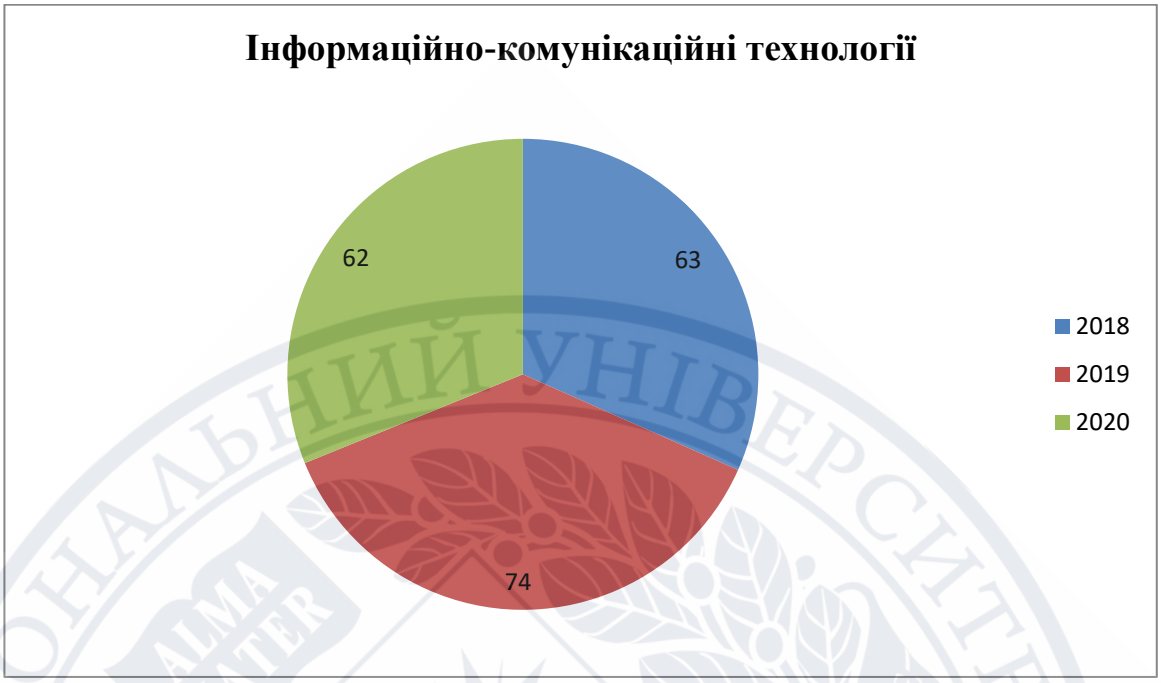

Рисунок 2.1. – Динаміка впровадження інформаційно-комунікаційних технологій

Згідно інформації на рисунку 2.1 можна стверджувати, що ІКТ 2020 року є каталізатором економічного зростання в епоху глобальних потрясінь. Україна займає 62 місце у світі й стабільно демонструє негативну динаміку розвитку [18, с. 103].

Безумовно, сучасні ІКТ формують людський капітал країни, що є основою для створення «інформаційного суспільства». Останніми трендами залучення ІКТ у повсякденне життя людства являється презентація сучасних освітніх програм у вільному доступі в глобальній Інтернет мережі. Це дозволяє різним верствам населення з різним рівнем достатку долучатись до освітніх процесів, оволодіти новими знаннями, вміннями та навичками, підвищити власний професіоналізм із максимальною користю для особистого трудового життя та мінімальними витратами. ІКТ можуть запропонувати країнам з різним рівнем економічного розвитку безпрецедентні можливості для зміни системи освіти.

Ключовими складовими ефективних комунікацій є дані, неопрацьовані цифри й факти, які відображають окремий аспект дійсності; а також інформація – дані, представлені у вигляді або формі, які мають змістові навантаження.

Інформація є особливо цінною, якщо вона достовірна, своєчасна, повна й доречна. А комунікативний процес – обмін інформацією між двома чи більше людьми.

Основна мета комунікативного процесу – забезпечення розуміння інформації, що є предметом обміну, тобто повідомлень. Однак сам факт обміну інформацією не гарантує ефективності її передачі. Тому попередньо треба мати уявлення про стадії процесу комунікації. Для вивчення матеріалу варто брати до уваги методи та засоби забезпечення безпеки інформаційних систем та комунікації (таблиця 2.3).

Таблиця 2.3. – Методи та засоби забезпечення безпеки інформаційних систем та комунікації

№	Політика для керування обліковими записами	Контроль безпеки паролів	Блокування облікових записів користувачів
1.	Політика паролів	Вимоги неповторності паролів	Граничне значення блокування
2.	Політика блокування облікових записів	Максимальний термін дії паролів	Блокування облікового запису користувача та тривалість блокування
3.	Політика «Kerberos»	Мінімальна довжина пароля	Скидання лічильника блокування

Захисту потребують інформація і дані, комунікаційні послуги і послуги з обробки та передачі даних, обладнання і засоби.

Згідно сучасних тенденцій, ІКТ надають навіть найменш розвиненим країнам можливості перетворення їх економік-аутсайдерів на інформаційні та високотехнологічні, тобто на ті, що спеціалізуються на продукції і з високою доданою вартістю, і які можуть конкурувати з передовими економіками на світовому ринку. Варто звернути увагу на те, що технологічні інновації сприяли глобалізації шляхом надання інфраструктури для встановлення транссвітових зв’язків. Революція, яка відбувається у сфері інформаційних і комунікаційних

технологій була і наразі залишається центральною і рушійною силою глобалізації сьогодення.

Незважаючи на безсумнівні переваги ІКТ, значні перешкоди для їх ефективного використання існують як в розвинених, так і у країнах, що розвиваються. Ці бар'єри мають бути елімінованими для повної реалізації потенціалу ІКТ. Деякі бар'єри є ендемічними (наприклад розрив між поколіннями, у процесах навчання, в отриманні досвіду у сфері ІКТ), а отже, подолати їх досить складно. Країни, що розвиваються стикаються з проблемами слаборозвиненої телекомунікаційної інфраструктури, низької комп'ютерної грамотності, відсутності обізнаності або низької спроможності користування мережею Інтернет. Сьогодні ІКТ має величезний вплив як для стрімкого соціально-економічного розвитку країни, так і для її повного занепаду.

Отже, крім того, комунікації можуть бути перервані перешкодою – шумом або розмовою людей поблизу. Перешкодами також є загублений на пошті лист, пошкодження телефонної лінії, невірна адреса електронної пошти тощо.

2.2. Можливості систем захисту інформації та комунікації

Роль ІКТ у сучасних умовах має величезне значення і у фінансіалізації країни. Будучи результатом досягнень сучасного науково-технологічного прогресу ІКТ обумовлюють його подальший розвиток. Вони все більше інтегруються у сферу науки як невід'ємні технічні складові більш глибокого та детального аналізу сучасних явищ та процесів.

Завдяки ІКТ відкриваються нові галузі в науці та техніці та відбувається органічна синергія класичних наукових шкіл. ІКТ сприяють вільному доступові до інформації. Завдяки ІКТ величезні масиви даних можуть не тільки швидко передаватись у різні куточки землі, але й швидко оброблятись, оновлюватись та сприяти створенню новітніх видів життєво необхідної продукції [31, с.157].

Простежимо можливості Panda Free Antivirus – системи захисту інформації та комунікації представлені на рисунку 2.2.

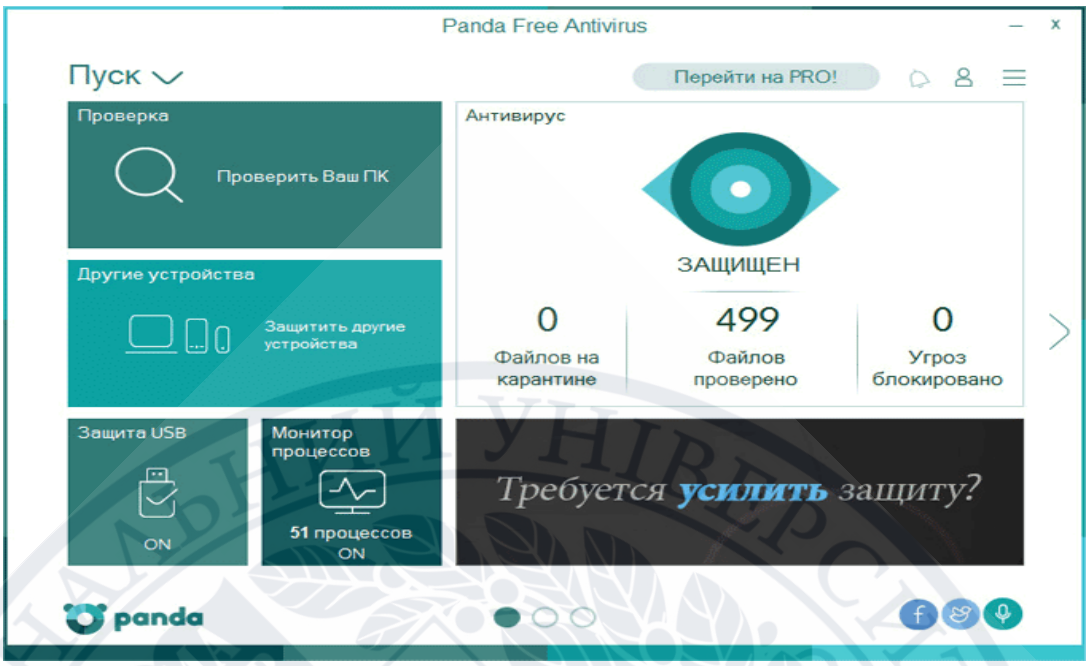

Рисунок 2.2. – Система захисту інформації Panda Free Antivirus

Деякі можливості ІКТ є основним стимулом заохочення соціально-економічного розвитку. Завдяки ІКТ, з одного боку, країни можуть швидко надолужити економічний розрив із світовими лідерами і отримувати величезну віддачу від створення додаткових матеріальних благ та робочих місць для висококваліфікованих робітників. З іншого боку, деякі країни розглядають розвиток і використання ІКТ в їх економіці та суспільстві як ключову компоненту їх національної стратегії з метою поліпшення рівня життя населення, збільшення рівня знань та посилення власної міжнародної конкурентоспроможності.

Сьогодні поширені такі типи комунікацій у організаціях: міжособові комунікації; комунікації в системах зв'язку та командах; комунікації в організаціях та електронні засоби комунікацій.

У сучасному інформаційному просторі злочин не потребує попередньої «обробки клієнта» та особистого контакту з потенційною жертвою. Головними інструментами стають комп'ютер і доступ до інформаційно-комунікаційних систем. За допомогою протизаконних програмних засобів одержується доступ до баз даних, банківських рахунків, автоматизованих систем керування. Елементи системи захисту комунікації представлено на рисунку 2.3 [36, с.100].

Рисунок 2.3. – Складові системи захисту комунікації

Одним з напрямів захисту інформації в комп'ютерних системах є технічний захист інформації (ТЗІ). В свою чергу, питання ТЗІ розбиваються на два великі класи задач:

1) захист інформації від несанкціонованого доступу (НСД)

2) захист інформації від витоку технічними каналами.

В комунікаційних системах використовуються такі засоби мережевого захисту інформації як міжмережеві екрани – для блокування атак з зовнішнього середовища [12, с.59]. Для доступу до інформації в даному випадку достатньо буде підключитися до цієї лінії або перехопити її в разі передачі комп'ютерної інформації по бездротових каналах зв'язку [26, с.138]. Можна, наприклад, побудувати макетну копію військового об'єкта, розмістити там макети техніки й імітувати діяльність щодо її технічного обслуговування, і це буде непрямою інформаційною атакою.

Для захисту від загроз в комп'ютерних системах реалізовують функції захисту, які у сукупності створюють так звані послуги безпеки. Кожна послуга, яка складається з набору функцій, протистоїть певній множині загроз конфіденційності, цілісності, доступності чи спостережуваності.

А можна за допомогою сучасних засобів ІКТ впровадити неправдиву або сплановану інформацію прямо в сховища інформації супротивника, щоб він при прийнятті командних рішень оперував неправдивими даними, і це буде прямою інформаційною атакою. Інформація, таким чином, виступає і як мета

впливу, і як зброя, а ІКТ при цьому розглядаються як зброя першого удару, руйнуючи або спотворюючи інформацію без видимих пошкоджень її носіїв [46, с.11].

Непряма інформаційна атака – спам, мережеві хробаки, трояни і інші (табл. 2.4).

Таблиця 2.4. – Моделі порушника та типи захисту інформації

Порушник			*Типи атак*
Кваліфікація	*Мотив*	*Технічна оснащеність*	Атаки відмови обслуговуванні Перехоплення й перенаправлення трафіку. Впровадження в комп’ютер шкідливих програм. Трояни Мережеві хробаки Віруси Шпигунські програми Спам
Початківець	Цікавість бажання оцінити свої можливості	Звичайний домашній комп'ютер	
Спеціаліст	Образа бажання помститися	Доступ до чужого комп’ютера	
Професіонал	Бажання збагатитися за рахунок не нанесення шкоди іншим	Потужний комп’ютер та програмне забезпечення	

Інформаційна війна переслідує такі основні цілі, як контроль інформаційного простору й забезпечення захисту своєї інформації від дій супротивника; використання контролю над інформаційним простором для проведення інформаційних атак на супротивника, або протистояння його діям щодо підвищення загальної ефективності державного управління шляхом ефективного впровадження інформаційно-комунікаційної техніки.

У західних наукових публікаціях це часто називають «knowledge society» — «суспільство, засноване на знаннях» або «суспільство знань» (в Україні більше використовують поняття «інформаційне суспільство»), і багато фахівців пропонують різні підходи щодо концепцій його створення [40, с.154]. Проте всі концепції головним ресурсом його розвитку визначають знання й інформацію органічно зв’язаними із розвитком ІКТ та систем штучного інтелекту.

Сьогодні засоби захисту комп'ютерної інформації забезпечують можливість здійснення контролю за збереженням **(**незмінністю, цілісністю) програмного забезпечення і баз даних; здійснюють спеціальне перетворення (шифрування) комп'ютерної інформації, що зберігається в зовнішніх запам'ятовуючих пристроях або переданої поміж технічними об'єктами, сигналізують про спроби несанкціонованого доступу до неї.

Разом із тим і в Україні несанкціоновані протиправні дії з комп'ютерною інформацією мають достатньо стійку тенденцію до зростання. Це дає підстави говорити про необхідність створення гармонійної і цілеспрямованої системи захисту комп'ютерної інформації. Причому в цьому процесі повинні брати участь фахівці не лише з формальних засобів захисту комп'ютерної інформації.

Недоліком усних комунікацій є те, що вони можуть бути недостовірними:

1. неправильно вибрані слова для вираження змісту;
2. перешкоди, що переривають процес;
3. слухач забуває частину або все повідомлення;
4. не вистачає часу на виважені відповіді тощо [31, с.129].

Письмові комунікації – звітами, документами та записами, тощо. Недоліком цих комунікацій є те що вони затримують зворотній зв'язок та взаємообмін, крім того вони складніші за усні й потребують більше часу. Переваги письмових комунікацій полягають у достовірності. Зазвичай їх використовують, коли одній чи обом сторонам потрібні письмові записи про те, що відбувалося [36, с.185].

Оскільки організація – система взаємно пов'язаних елементів, а керівництво повинно добиватися, щоб мати спеціалізовані елементи працювали пов`язано для просування організації в необхідному напрямі.

Стиль життя XXI століття передбачає часте використання інформаційних технологій та гаджетів. З ростом використання смарт-пристроїв, зростає і небезпека витоку та втрати даних. Кожен користувач повинен подбати про належний рівень безпеки (кібербезпеки) цифрових пристроїв і інформації.

Так, наприклад, виділяють два основні рівні захисту смартфона:

– фізичний захист – базові правила догляду за смартфоном (не залишати без нагляду, не вводити код доступу на очах у інших людей). Є небезпека «зламу» девайса та використання його у власних інтересах (спустошити рахунки, отримати персональні дані, видалити інформацію);

– захист «начинки» – операційної системи, програм та застосунків. Існує безліч способів захисту смартфона на «внутрішньому» рівні (вчасне оновлення операційної системи, використання багатофакторної аутентифікації та складних паролів).

Можна також навести основні правила кібербезпеки користувачів сучасними технічними засобами:

•*вчасне оновлення операційної системи пристрою:* компанії-виробники постійно оновлюють софт, а оновлення найчастіше виправляють усі виявлені вразливі місця операційних систем, запобігають витоку даних користувача, блокують несанкціоновані доступи тощо; 90 % оновлень усіх операційних систем включають поліпшення заходів безпеки, адже компанії постійно моніторять і знаходять все більше і більше вразливих місць в своїх же ОС. Все частіше в системних оновленнях на перший план виходить безпека: – віддалене налаштування великої кількості пристроїв та їх адаптація до конкретних потреб; – одночасне додавання тисяч пристроїв в ЕММ без необхідності вручну реєструвати кожен пристрій; – просте керування безліччю пристроїв за допомогою хмарного рішення ЕММ; – застосування комплексних функцій захисту та керування для корпоративних пристроїв; – керування версіями ОС на мобільних пристроях для максимальної економічної ефективності.

•*використання складних паролів та менеджерів паролів*: не застосовувати однакові паролі для різних сервісів; обирати важкі паролі, які складаються з комбінації різних символів та чисел; доступ до персональної інформації відбувається через аналіз профілю в соціальних мережах (соціальна інженерія); користуватися менеджером паролів;

•*використання багатофакторної аутентифікації:* двофакторна або багатофакторна аутентифікація;

•*використання біометричного захисту*: використання відбитку пальців або сканування особистості (faceID для IOS); блокування доступу до телефону не лише через паролі і пін-коди; біометрична ідентифікація – надійний і комфортний інструмент;

•*встановлення ПЗ і застосунків лише з офіційних джерел*: самі ОС, не дозволяють або попереджають про небезпеку інсталювати певний софт; безпечним є скачування додатків з офіційних сайтів виробника;

•*користування лише відомими, безпечними Wi-Fi мережами*: відкриті, загальнодоступні мережі Wi-Fi небезпечні для використання; шахраї можуть отримати доступ до електронної пошти, акаунтів у соціальних мережах, персональних даних та навіть банківських карток; слід користуватися мобільними даними в загальнодоступних місцях або користуватися VPN;

•*встановлення додаткового захисту*: антивірусне програмне забезпечення; зберігати дані у безпечній хмарі, ізольованій від решти системи;

•*постійне увімкнення геолокації:* не відключати геолокацію, з допомогою додаткових сервісів у будь-який момент можна виявити гаджет, активувати функцію, заблокувати пристрій і видалити всі особисті дані на ньому.

Загалом способів захистити власні технічні засоби комунікації та убезпечити свою комунікаційну діяльність існує чимало. Проте, можливості систем захисту інформації та комунікації сьогодні потребують постійного удосконалення та розвитку .

2.3. Автоматизація систем захисту інформації та комунікації

Інформаційна безпека характеризується ступенем захищеності інформації, стійкістю основних сфер життєдіяльності економіки, науки, техносфери, галузі управління, військової справи, суспільної свідомості, відношення до небезпечних (дестабілізуючих, деструктивних, суперечних інтересам країни тощо) інформаційних впливів, причому як до впровадження, так і до вилучення інформації.

Автоматизація систем захисту безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають. Інформаційні технології (ІТ) включають в себе широкий обсяг дисциплін і сфер діяльності і стосуються технічних засобів обробки і передачі даних чи інформації [18, с.159-160].

Основні потенційні загрози на окремо взятому комп'ютері такі: − інформацію можна підглянути, порушивши у такий спосіб її конфіденційність; − інформацію можна підмінити, порушивши її цілісність; − доступ до інформації може бути заблоковано, отже порушується доступність інформації та послуг, надаваних комп'ютером; − понад зазначене існує небезпека того, що реалізовування загрози залишиться таємним, або провину буде покладено на непричетну до цього особу. Це є порушення спостережуваності дій користувача або поводження системи.

Для захисту від загроз в комп'ютерних системах реалізовують функції захисту, які у сукупності створюють так звані послуги безпеки.

На першому рівні – захисту підлягають ІР: масиви інформації у різних предметних сферах, бази моделей, бази і банки даних у відповідних інформаційних системах.

На другому рівні – передбачається захист функціональних апаратних та програмних елементів конкретної ІС для завдань управління.

Третій рівень – передбачає захист ІР, які протікають в ІС: сприйняття/ збір/ відбір, оброблення, зберігання, представлення, передавання інформації, які формують інформаційний зміст фаз, операцій та оброблення даних.

Четвертий рівень – передбачає захист ІМ (К) відповідно до їх класифікації та топології для ІАС, АСУ, САО, СППР.

На п'ятому рівні – передбачається управління об'єктом – життєвим циклом інформації, яка функціонує в ІС та управління комплексною системою безпекою ІТ. Розглянемо модель системи захисту інформації та комунікації на рисунку 2.4 [51].

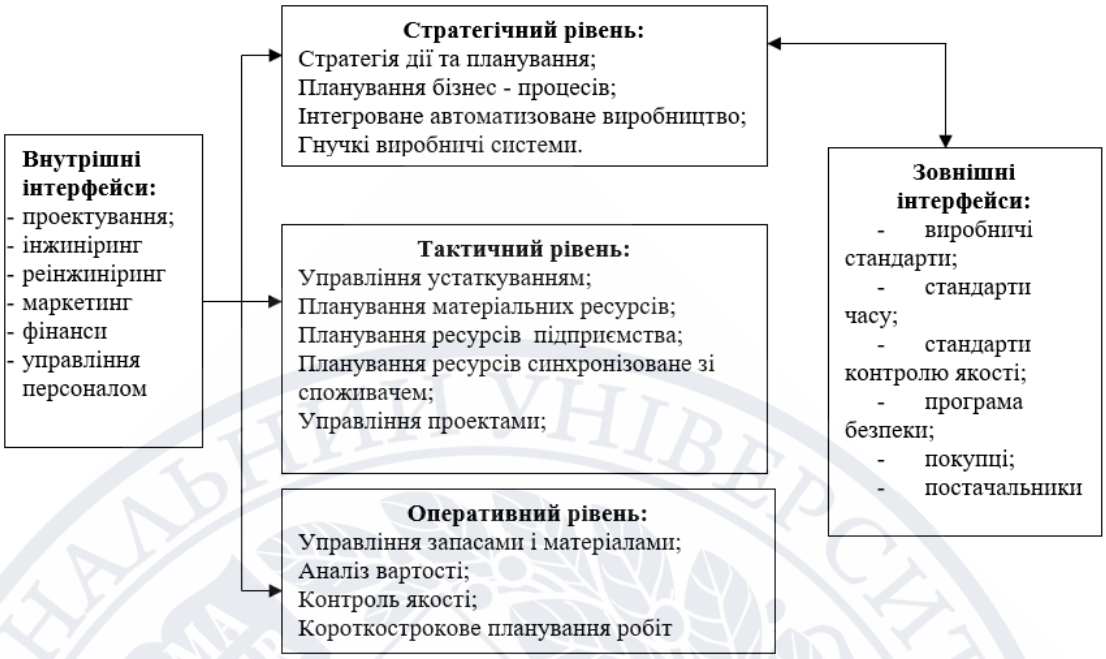

Рисунок 2.4. – Модель системи захисту інформації та комунікації

Поняття власне інформаційної безпеки стосується безпечності процесу технічної обробки інформації і є властивістю функціонально безпечної системи. Така система повинна унеможливлювати несанкціонований доступ до даних та запобігати їхній втраті у разі виникнення збоїв.

Розглянемо діалогове вікно автоматизованої системи захисту інформації та комунікації програмою Kaspersly Free (рисунок 2.5).

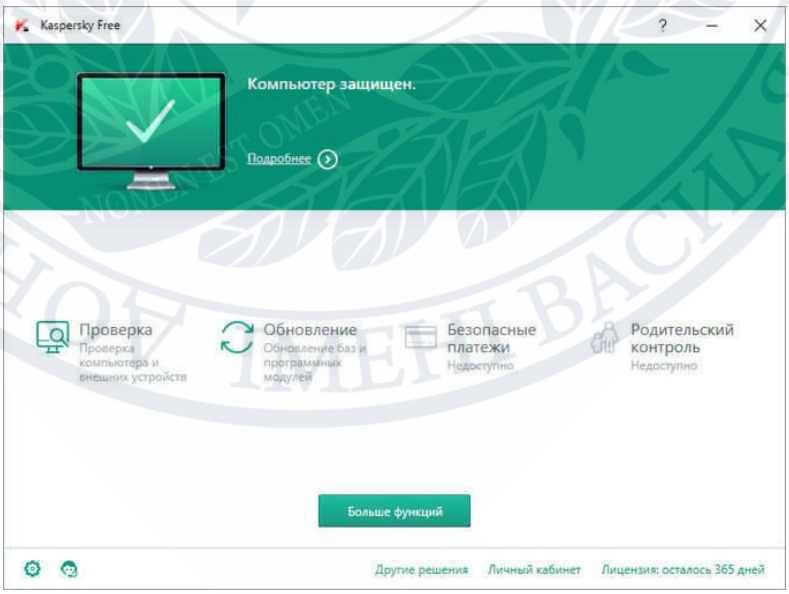

Рисунок 2.5. – Діалогове вікно захищеного комп’ютера програмою Kaspersly Free

Говорячи про інформаційну безпеку часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору інформаційна безпека – це економічний параметр, який повинен враховуватися у роботі підприємства, а інформацію, можна розглядати як певний товар або цінність, що підлягає захисту, а відтак вона має бути доступною лише для авторизованих користувачів чи програм [34, с.201 -202].

Для характеристики основних властивостей інформації як об'єкта захисту часто використовується модель CIA [47]: 1) конфіденційність — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем; 2) цілісність — означає неможливість модифікації неавторизованим користувачем; 3) доступність — властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час [44, с.80].

Інформаційна безпеки особи характеризується як стан її захищеності, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору. Розглянемо динаміку захисту інформації та комунікації на рисунку 2.6.

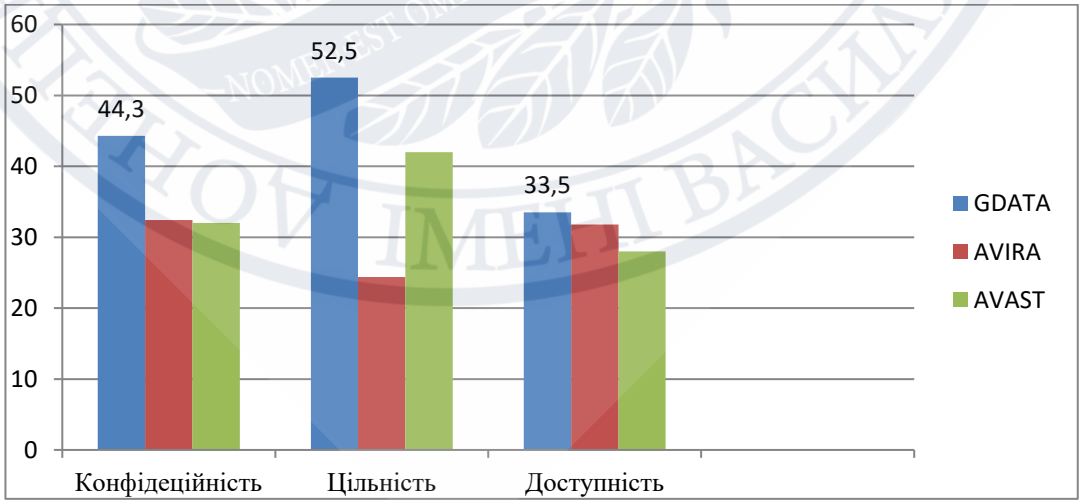

Рисунок 2.6. – Розглянемо динаміку захисту інформації та комунікації

Тут простежується захист інформації та комунікації, а гарантування інформаційної безпеки включає в себе законність інтересів особи.

Ефективне виявлення порушника інформаційної безпеки в інформаційно-комунікаційних мережах та системах є складною задачею, що потребує використання спеціальних засобів захисту – систем виявлення порушника. Більшість таких систем ґрунтуються на застосуванні сигнатурних методів, що мають ряд недоліків.

Тож можна виділити низку основних помилок, яких слід уникати під час налаштування захисту від несанкціонованого доступу до ресурсів та інформації:

1) слабкі паролі, які складаються із коротких слів і фраз, не містять цифр та інших символів;

2) використання відкритих (нешифрованих) способів передавання даних;

3) застарілі версії програмного забезпечення з відомими та неусунутими вразливостями;

4) використання віддаленого доступу до ресурсів та систем управління обладнанням з використанням загальних каналів мережі Інтернет.

Для захисту веб-додатків потрібно використовувати мережеві екрани. Якщо поєднати новітнє спеціальне обладнання та елементарні правила безпеки користування інформаційними носіями, то, можливо, нам і вдасться досягти певних результатів [50, с.351].

Отже, нині неможливо створити систему, захист якої не можна буде зламати, основним принципом може бути створення такого механізму захисту, вартість злому якого буде дорожчою за інформацію, яку можна отримати Сьогодні впровадження програмних засобів безпеки є необхідним для збереження інформації і для виконання функцій захисту. В сучасних умовах, нажаль не гарантуючи належний захист інформації, це не можливо забезпечити через стабільний економічний розвиток окремих підприємства чи держави.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

3.1. Необхідність захисту інформації органів влади та персональних даних

В умовах стрімкого розвитку інформаційного суспільства, активного формування різноманітних комунікаційних мереж, становлення різних форм самоорганізації населення, в тому числі громадянських рухів, союзів, асоціацій тощо, неабиякого значення набувають питання створення ефективної системи комунікації між владою і суспільством, що сприяє підвищенню результативності державного управління і забезпеченню сталого соціально-економічного розвитку. У процесі взаємодії органів влади та суспільства виникає потреба захисту інформації та створення безпечного середовища комунікації (Додаток Б). Об’єктом взаємодії виступає конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом. Так, захисту підлягає відкрита інформація, яка є власністю держави і у Законі України «Про інформацію» [5] належить до статистичної, правової, соціологічної інформації та інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів чи органів місцевого самоврядування, секретної конфіденційної інформації [31, с. 198].

Одним із найважливіших пунктів захисту інформації є захист від вірусів. Комп’ютерний вірус це невеличка програма, яка може самопоширюватися. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані [24, с. 167].

З метою запобігання поширенню вірусів в системі роботи Могилів-Подільської районної ради на кожному персональному комп’ютері встановлено антивірус та firewall. Але велика кількість програмного забезпечення слабо працездатна, а що б обрати потрібний продукт слід провести спеціальний аналіз.

Так, у роботі персоналу органу влади на персональних комп’ютерах використано такі чотири антивірусні програми:

1) Avast! Proffesional Edition 4.8
2) AVIRA AntiVir Premium 8.2.
3) ESET NOD32 Antivirus 3.0
4) G DATA Antivirus 2009.

Головним результатом роботи антивірусу є відсоток виявлення шкідливих програм. П’ять найкращих антивірусів та їх відсоток виявлення шкідливих об’єктів на прикладі роботи організації представлено у таблиці 3.1.

Таблиця 3.1. – Антивіруси та відсоток виявлення шкідливих об’єктів в роботі з інформацією Могилів-Подільської районної ради

№	Назва програмного продукту	Відсоток виявлення шкідливих об’єктів
1	G DATA	99.8
2	AVIRA	99.7
3	McAfee	99.1
4	Symantec	98.7
5	Avast	98.2

Тож для безпечної роботи комп’ютерів слід вибирати програмне забезпечення з першої п’ятірки програм [12, с.173]. Впровадження антивірусної програми криптографічного захисту інформації показано на рисунку 3.1.

Рисунок 3.1. – Структура антивірусної програми та її функції [17, с. 68]

Антивірусні програми можуть виконувати такі основні дії: сканування пам’яті та вмісту дисків за розкладом та сканування пам’яті комп’ютера, а також файлів, що записуються та читаються, під час виконання операцій з ними, автоматичне оновлення антивірусних баз через Інтернет.

У роботі Могилів-Подільської районної Ради використовують такі антивірусні програми: програми-детектори, програми-лікарі та інші. Розглянемо діалогове вікно Обзор G Data Internet Security 2016 (25.1) (рис. 3.2).

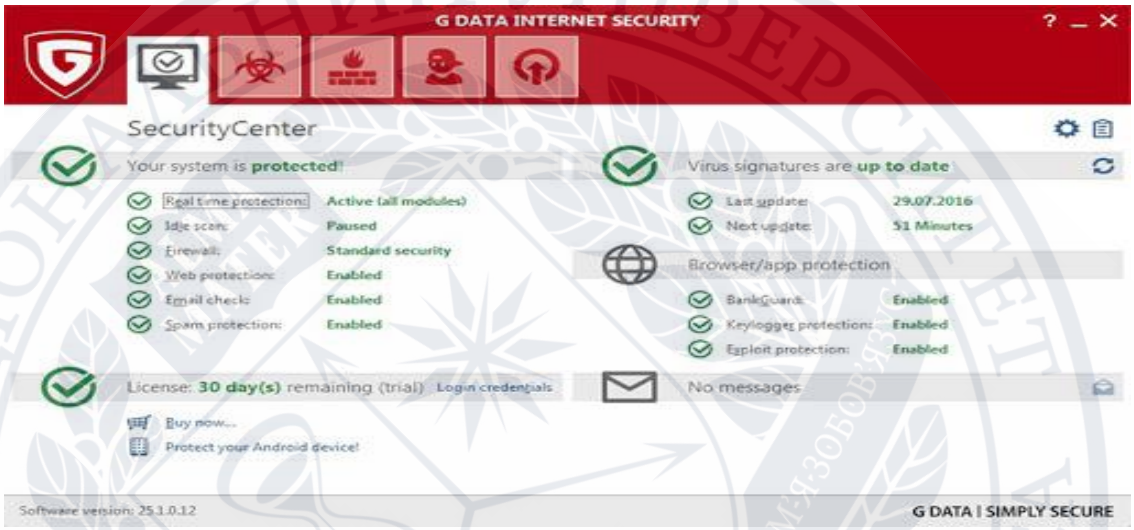

Рисунок 3.2. – Діалове вікно Обзор G Data Internet Security 2016 (25.1)

Районна рада для працівників адміністрації використовувала антивірусну програму Norton Security хороша проргама, яка оновлює версію 25.0 до 25.1.

Також антивірусні програми можуть бути як поліфагами, так і спеціалізованими, як наприклад програми-ревізори призначені для виявлення зараження вірусом файлів, а також знаходження ушкоджених файлів. Ці програми запам’ятовують дані про стан програми та системних областей дисків у нормальному стані (до зараження) і порівнюють ці дані у процесі роботи комп’ютера.

Захист інформації методом криптографічного перетворення полягає у приведенні її до неприйнятного увазі шляхом перетворення складових частин інформації (букв, цифр, складів, слів) за допомогою спеціальних алгоритмів, апаратних засобів і кодів ключів. Ключ тут – це змінна частина криптографічної системи, що зберігається в таємниці і визначальна, шифрувальне перетворення якого виконується в даному випадку.

Раніше в роботі установи ефективно застосовувалася антивірусна програма Avast! Professional Edition 4.8 (рисунок 3.3).

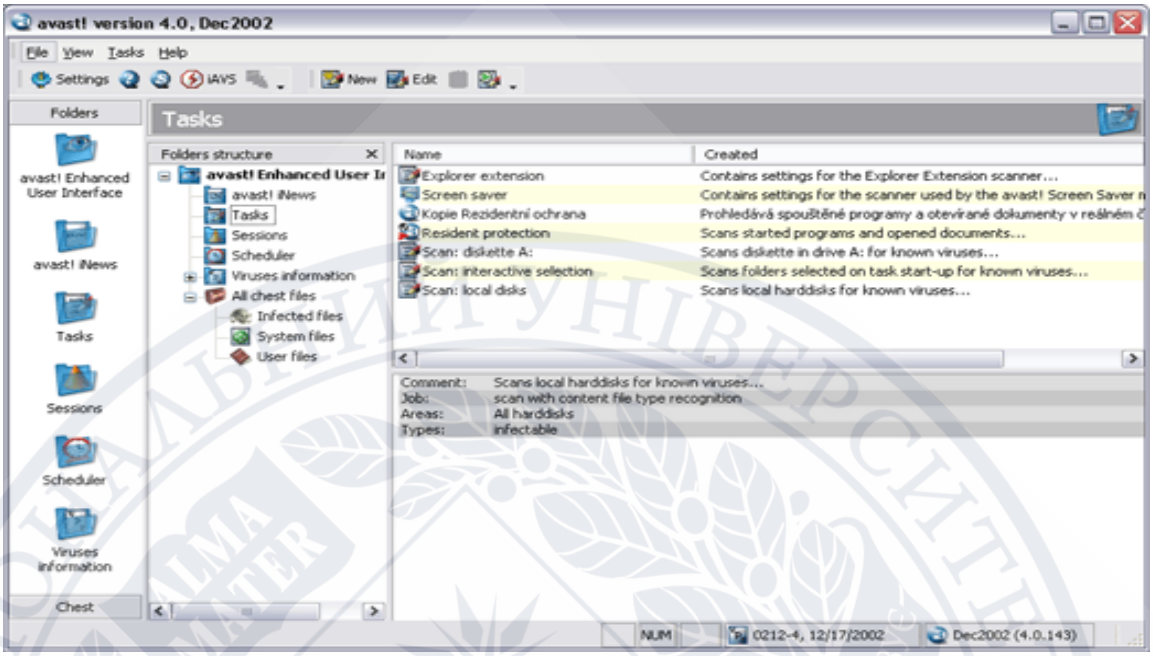

Рисунок 3.3. – Діалогове вікно Avast! Professional Edition 4.8

Проте, встановлено, що не слід використовувати механізм Avast! антивірусного захисту, заснований на високоефективній технології. Використовуючи швидкі та ефективні оновлення та вдосконалений багаторівневий захист від усіх джерел зараження в режимі реального часу Avast! завжди треба охороняти свій комп'ютер. Avast! 4 Professional Edition поєднує в собі всі високопродуктивні технології для досягнення однієї мети – забезпечити найвищий рівень захисту від комп'ютерних вірусів. Цей продукт є ідеальним рішенням для робочих станцій на базі Windows.

У роботі з інформацією Могилів-Подільської районної ради використовувалося програмне забезпечення Microsoft Project. В наступному підрозділі у таблиці 3.2 зазначено ресурси, необхідні для виконання проекту.

У цьому напрямі проведено детальний аналіз систем безпеки інформації в роботі Могилів-Подільської районної ради, охарактеризовано його види діяльності, подано аналіз основних завдань усіх відділів та філій. Проаналізовано технічне та програмне забезпечення. Розглянуто основні вид документообігу Могилів-Подільської районної ради та схему корпоративної мережі, яка використовує Avira AntiVir (рисунок 3.4).

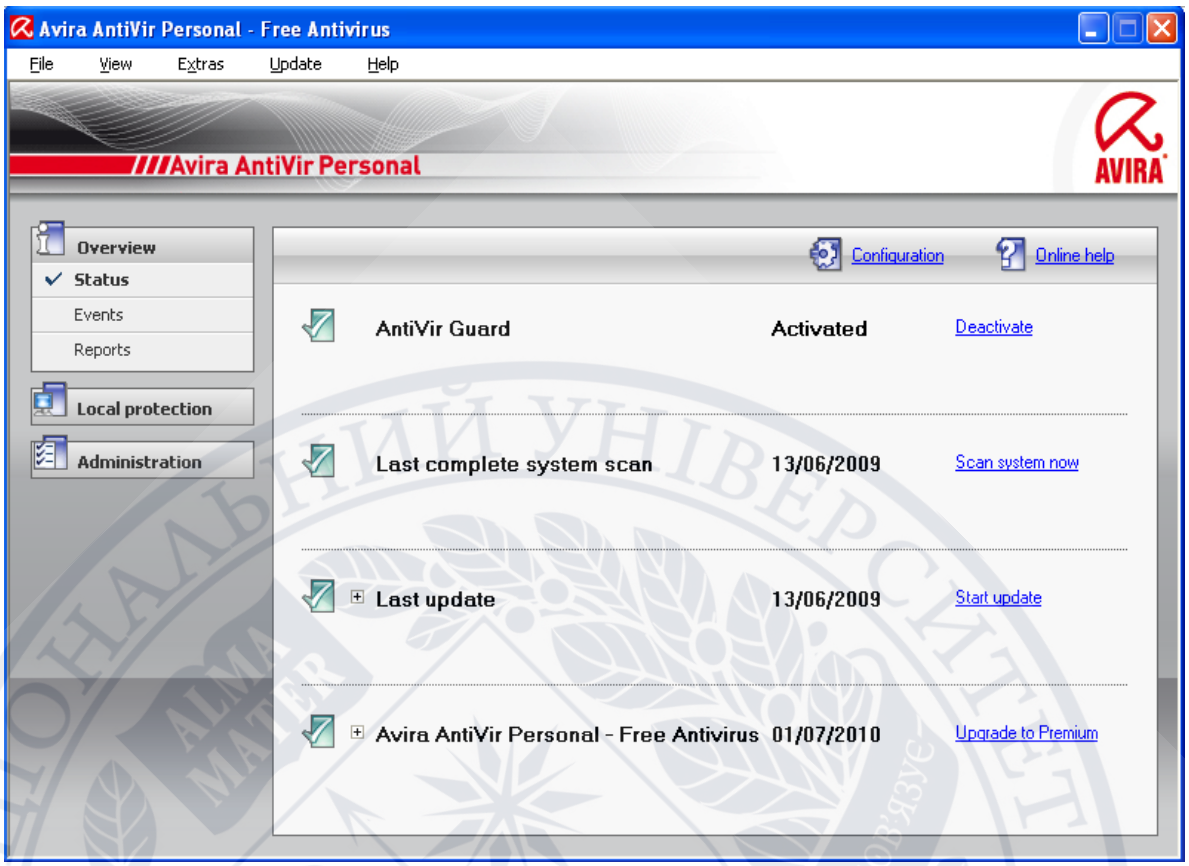

Рисунок 3.4. – Антивірусна програма Avira AntiVir

Отже, Avira Antivirus – серія антивірусних програм від німецької компанії Avira GmbH. Всі продукти серії засновані на антивірусному двигуні Luke Filewalker, у якій значно покращену версію продукту, завдяки чому швидкість сканування збільшилась на 20 відсотків.

Подібна ситуація в роботі з персональною інформацією і потреби використанням систем захисту інформації спостерігається в роботі сучасних застосунків, які активно використовують громадяни. Зокрема застосунок Дія, який вміщує всі особистісні документи і є важливим у інформаційно-комунікаційній діяльності України в межах реалізації програми діджиталізації. Найбільш актуальне питання щодо мобільного застосунку Дія –захист персональних даних користувачів. Користувачі усвідомлюючи важливість захисту персональних даних очікують від розробників відповідальність перед українцями-користувачами застосунку. Виникають головні запитання щодо безпеки використання цифрових документів і унеможливлення витоку даних.

В свою чергу, розробники гарантують, що Застосунок Дія не зберігає персональних даних користувачів, а лише разовий запит ідентифікованого громадянина відображає інформацію з реєстрів. Через Дію неможливо оцифрувати документи чи завантажити їх. На смартфонах Android нереально зробити скрін із застосунку. Дія – це винятково віддзеркалення вже наявних у громадян документів.

Архітектура застосунку Дія побудована таким чином, що на серверній частині взагалі не здійснюється зберігання персональних даних користувачів. При цьому інформація в каналах передачі даних передається у зашифрованому вигляді, а на деяких етапах – використовується подвійне шифрування. Усі сервери мобільного застосунку Дія розташовані в Україні, тобто ніяка інформація про користувачів не йде за кордон. Серверна частина системи розгорнута в хмарній інфраструктурі, яка має необхідні сертифікати безпеки, у тому числі Комплексна система захисту інформації (КСЗІ). Єдине місце, де було залучено зарубіжну компанію, – це захист від атак розподіленого доступу (DDOS-атак). Для цього було використано інфраструктуру компанії Amazon, яка частково розташована в Німеччині. Крім того, мобільний застосунок Дія пройшов низку позитивних аудитів – як приватних, так і державних (ДССЗЗІ).

Захист персональних даних у мобільному застосунку Дія представлено у вигляді кращих практик безпеки рішень такого типу – використано підхід «глибокого захисту» (defense-in-depth). Проведено відповідні пен-тести – тестування безпеки застосунку компанією EPAM.

Важливим моментом захисту інформації є тестування технологій захисту. Застосунок тестувала внутрішня команда EPAM, яка не була залучена до її розробки. Це був новий, незнайомий продукт, що дозволило зберегти об’єктивність дослідження. Всього близько 20 експертів із кібербезпеки, фахівці EPAM Security Competence Center, перевіряли і production backend, і мобільний застосунок. Також разом із компанією EPAM команда Дії проводила тестування, до якого залучали білих хакерів, щоб виявити вразливі місця. Така всебічна перевірка гарантує надійність та захищеність документів користувачів.

У процесі ідентифікації застосунок потребує перевірки через банківський застосунок. А чи можливо отримати персональні дані та доступ до банківських рахунків через BankID, і чи не стає вся інформація повністю доступною кіберзлочинцям. Встановлення Дії передбачає ідентифікацію за допомогою технології BankID. Через BankID зловмисники не зможуть дістати доступ до банківських рахунків, оскільки банки зберігають про користувачів два типи інформації: personal identifiable information (PII) – і personal credit card information (PCI). За вимогами безпеки ці дані зберігаються окремо і з різними API. Для роботи застосунку Дія користувач надає доступ суто до personal identifiable information (PII). Усі банки, що належать до системи BankID Національного банку України, у тому числі Приватбанк, повідомляють, до яких саме даних буде відкрито доступ, і лише сам користувач може надати згоду на передачу цієї інформації про себе (ПІБ, паспорт, ІНН, телефон, адресу і електронну пошту). Перевірити цей перелік можна на сайті https://id.gov.ua. Отримана інформація передається на смартфон користувача у вигляді зашифрованого і підписаного криптопримітиву. Він не розшифровується на пристрої, а лише слугує ключем, за яким застосунок отримує доступ до документів.

Окремої уваги потребує захист та безпека передачі інформації через QR-код. Користувачам відомо, що для того щоб перевірити достовірність документів у Дії, використовується QR-код. У QR-коді зашифрований одноразовий пароль, який дозволяє верифікувати документ і дійсний лише три хвилини. Ризик того, що хтось устигне сфотографувати код, скористається ним упродовж трьох хвилин і так дістане доступ до документа мінімальний.

Беручи до уваги вище сказане, можна відмітити високий рівень безпеки державного застосунку інформаційно-комунікаційної діяльності та техніко-технологічні можливості захисту персональних даних користувачів ІКД.

Загалом інформація та комунікаційні технології створюють інформаційно-комунікаційний простір. Це специфічна форма існування інформаційних систем, яка забезпечує й стимулює оперативні інформаційні взаємодії

виробників інформації та її споживачів, трансляцію знань, накопичених в інформаційних ресурсах, і їхнє збереження в сформованій інформаційній інфраструктурі, сукупність комунікаторів, реципієнтів, значеннєвих повідомлень, комунікаційних каналів і засобів комунікації. Проте будь-які системи захисту повинні проходити регулярне оновлення і вдосконалення, що суттєво підвищить безпеку інформації користувача та зробить віртуальне життя і комунікацію на різних рівнях прозорою і захищеною.

3.2. Використання технічних і технологічних засобів захисту у роботі з інформацією

У роботі з інформацією в роботі досліджуваного органу влади було впроваджено захист інформації за такими основними напрямками: технічні засоби безпеки в організації, ведення паролів до всіх технічних та програмних засобів, введення електронних підписів для всіх відділів, філій та осіб. Саме ж управління процесом шифрування здійснюється за допомогою періодично змінюваного коду ключа, що забезпечує оригінальне представлення інформації при використанні одного і того ж алгоритму або пристрою. Знання ключа дозволяє відносно швидко, просто і надійно розшифрувати дані. Однак без знання ключа ця процедура може виявитися практично нездійсненною навіть при використанні комп’ютера (табл. 3.2) [18].

У роботі Могилів-Подільської районної ради відбулися такі нововведення. Встановлена система резервного копіювання, що значно знизила ризик втрати цінної інформації; проведений аналіз антивірусного програмного забезпечення та найкращий варіант встановлено на всіх персональних комп’ютерах. Введено систему криптографічного кодування інформації, після якого підприємство перейшло на новий рівень захисту при передачі інформації.

Таблиця 3.2. – Технічне та програмне забезпечення роботи Могилів-Подільської районної ради

Бухгалтерії	Технічні відділи	Директори та головні менеджери	Wed-відділ	Сервіс центр
Прикладні програми	Програма 1С бухгалтерія Outlook Express, Internet Explorer, Microsoft Office	Outlook Express, Internet Explorer, Microsoft Office	Outlook Express, Internet Explorer, Microsoft Office	Web-сервери Microsoft Office,1С «Підприємство»
Спільно використовувані ресурси	Принтери: CANON LBP 2900 Ксерокс: Canon FC-108	Принтер: CANON LBP 2900 Сканер: Mustec 2448	Сканер: Mustec 2448	Принтер: CANON LBP 2900 Ксерокс: Canon FC-108
Операційна система	Windows XP	Windows XP	Windows XP	Windows XP, Linux
Кількість комп'ютерів	2	10	9	2

Ще одне важливе впровадження систем захисту McAfee Internet Security, який має функцію безповоротного видалення даних та налаштування оптимальної роботи ПК (рис. 3.5) [15, с. 33].

Рисунок 3.5. – Антивірус McAfee Internet Security

Система онлайн резервного копіювання дозволяє зберігати найбільш важливі файли в мережі, на випадок їх пошкодження або видалення. Для цих цілей доступно 1 ГБ онлайн простору. Модуль QuickClean очищає операційну

систему від непотрібних і застарілих файлів, збільшуючи при цьому її продуктивність.

У антивірусу є функція незворотного видалення конфіденційних файлів, які буде не можна відновити спеціальними програмами для відновлення файлів на жорсткому диску.

Основні можливості McAfee Internet Security:

— забезпечення антивірусного захисту від програм-шпигунів, шкідливих додатків, підозрілих сайтів;

— наявність двостороннього брандмауера;

— швидке завантаження файлів, їх сканування;

— функція безповоротного видалення даних;

— можливість перевірки USB-носіїв та інших пристроїв знімного типу [4, с. 62].

Функція анти-спаму для попередження отримання небажаних поштових повідомлень, можливість батьківського контролю є резервне копіювання.

Пошук та інсталяція останніх оновлень для Windows і інших програм на ПК. Перегляд комп’ютерів і інших пристроїв, підключених до мережі. Можливість віддаленого виявлення і блокування втраченого мобільного пристрою, видалення інформації на ньому.

Функція «Моя домашня мережа» дозволяє переглядати комп’ютери та пристрої, підключені до домашньої мережі, усуваючи проблеми безпеки на комп’ютерах, з встановленими антивірусами McAfee. Модуль SiteAdvisor надає інформацію про безпеку відвідуваних веб сайтів.

Варто зазначити, що після цих нововведень у роботі Могилів-Подільської районної ради повинно спостерігатись покращення захисту інформації та кращої та стабільної роботи з інформацією на підприємстві.

Таким чином, антивірусна програма має простий, зручний та інтуїтивно зрозумілий інтерфейс. Для ознайомлювальних цілей антивірус пропонує безкоштовне користування протягом 30 днів.

3.3. Реалізація механізмів захисту інформації у роботі Могилів-Подільської районної ради

Впровадження систем захисту інформації у Могилів-Подільської районної ради передбачає реалізацію та вироблення ефективних заходів, пропозицій і рекомендацій керівництву підприємства, спрямованих на недопущення витоку конфіденційної інформації про діяльність підприємства і проведені роботи.

Підробка комп'ютерної інформації – злочин, який можна вважати різновидом несанкціонованого доступу з тією різницею, що скоїти його може і стороння особа, і законний користувач, і розробник 1С. В останньому випадку може підроблятись вихідна інформація з метою імітування робото здатності 1С і здачі замовнику свідомо несправної продукції. До подібного виду злочинів можна віднести підтасування результатів виборів, голосувань і інше [12, с. 176].

Введення у програмне забезпечення «логічних бомб» – невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Це ще одна можливість втручання в роботу установи і загроза інформації.

Завдання захисту інформації Могилів-Подільської районної ради:

1) обробка й зберігання конфіденційних документів;

2) контроль системи конфіденційного документообігу (у не дуже великих організаціях доцільно організувати СКЗІ в такому складі: начальник СКЗІ; співробітник, що займається програмно-апаратним захистом);

3) запобігання несанкціонованому доступу (НСД) до інформації;

4) запобігання витоку інформації за рахунок побічних електромагнітних випромінювань (ПЕМВ);

5) захист інформації від комп'ютерних вірусів;

6) захист інформації від збоїв у системі живлення;

7) захист від копіювання;

8) програмний захист каналів передачі даних.

Функції конфіденційного діловодства у роботі установи варто покласти на вже наявних співробітників, котрим на цей час доручено створення й обробка документів, що містять конфіденційну інформацію.

У 2019 році у роботі Могилів-Подільської районної ради було розроблено важливий документ гарантування безпеки інформації та відповідальність за її порушення – Положення про порядок експлуатації локальної мережі адміністрації. Цей документ став основою забезпечення захисту електронної інформації, яка обробляється в органах влади Вінницької області (Додаток А).

Регулярно здійснюється робота з інсталяції та налаштування спеціалізованого програмного забезпечення, проводяться аудити інформаційної безпеки в управліннях, сканування на пошук вразливостей, роботи з виявлення та локалізації комп'ютерних вірусів, розроблення інструкцій, положень та рекомендацій щодо організації робіт із забезпечення інформаційної безпеки.

Простежимо механізм комплексу заходів захисту інформації на об'єктах інформаційної діяльності Могилів-Подільської районної ради (рис. 3.6) [2, с. 37].

Рисунок 3.6. – Система антивірусного захисту інформації

Центром розбудовано комплексну систему антивірусного захисту в інформаційно-телекомунікаційній системі органів виконавчої влади та місцевого самоврядування, забезпечено її повсякденне функціонування.

Враховуючи важливість забезпечення захисту інформації, постійно проводиться роз’яснювальна робота із співробітниками структурних підрозділів органів виконавчої влади та місцевого самоврядування. Для підвищення рівня якості робіт Центром періодично проводяться семінари та навчання з особами, відповідальними за захист інформації в структурних підрозділах. Співробітники Центру розробляють повний комплект документів, необхідний для проходження державної експертизи комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.

Окремо варто зупинитися на етапах розробки концепції захисту інформації та її реалізації в роботі з інформацією (рис. 3.7).

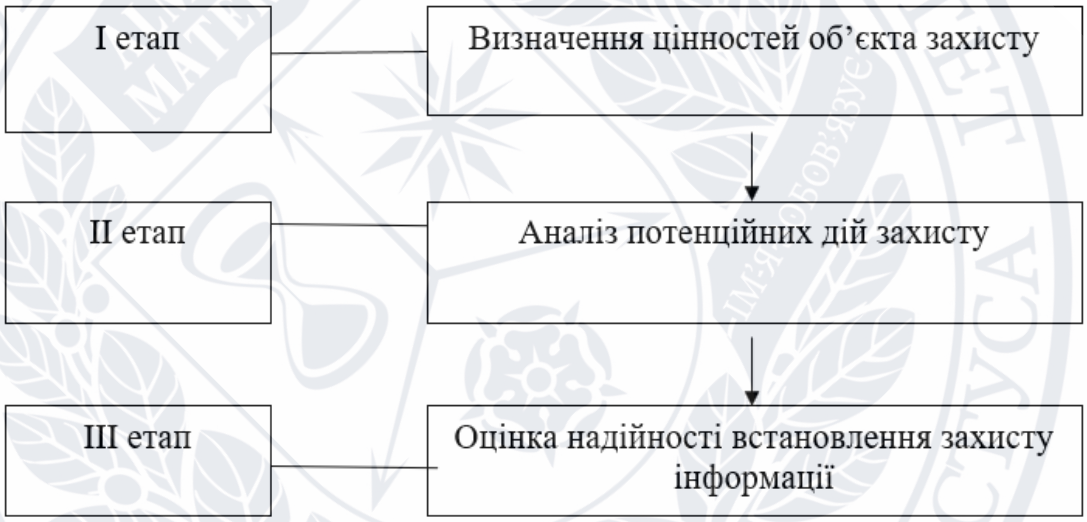

Рисунок 3.7. – Етапи розробки концепції захисту інформації [16, с. 258]

На рисунку можна простежити, що робота і вдосконалення системи захисту інформації Могилів-Подільської районної ради реалізована у три етапи. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів, як інформаційне шпигунство, саботаж, крадіжки зі зломом. Далі потрібно проаналізувати найбільш ймовірні дії зловмисників стосовно основних об’єктів, що потребують захисту. Головною метою третього етапу є аналіз обставин, у тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту. Концепція захисту повинна містити перелік організаційних, технічних і інших заходів, що забезпечують максимальну безпеку.

Політика захисту є загальним документом, де перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту. Власне документ складається із декількох сторінок тексту. Він формує основу фізичної архітектури мережі, а інформація, що знаходиться в ньому, визначає вибір продуктів захисту. При цьому, документ може і не включати список необхідних закупок, але вибір конкретних компонентів після його складання повинен бути очевидним.

Рисунок 3.8. – Вимоги в організації роботи з інформацією

Під час свого існування органом влади здійснено значний обсяг робіт, спрямованих на підвищення рівня захищеності інформації в інформаційно-телекомунікаційній системі органів виконавчої влади та місцевого самоврядування області, а також забезпечення безпеки інформації у режимних приміщеннях (рис. 3.8) [20].

Для виконання цих робіт Комунальне підприємство Обласний інформаційно-аналітичний центр (далі - КП ОІАЦ) має режимно-секретний орган, спеціальний дозвіл Служби безпеки України на провадження діяльності, пов’язаної з державною таємницею, ліцензію Адміністрації Державної служби спеціального зв’язку та захисту інформації України на надання послуг у галузі технічного захисту інформації.

Центром розбудовано комплексну систему антивірусного захисту в інформаційно-телекомунікаційній системі органів виконавчої влади та місцевого самоврядування, забезпечено її повсякденне функціонування.

Враховуючи важливість забезпечення захисту інформації, постійно проводиться роз'яснювальна робота із співробітниками структурних підрозділів органів виконавчої влади та місцевого самоврядування. Надаються необхідні консультації, практичні рекомендації щодо ефективного використання технічних засобів та програмного забезпечення.

Отже, співробітники Центру розробляють повний комплект документів, необхідний для проходження державної експертизи комплексної системи захисту інформації в інформаційно-телекомунікаційних системах в діяльності Могилів-Подільської районної ради. Загалом, органи виконавчої влади, які мають дозвіл на провадження діяльності з технічного захисту інформації, вправі за згодою Державної служби спеціального зв'язку та захисту інформації України організовувати проведення державної експертизи комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах на підприємствах, в установах та організаціях, які належать до сфери їх управління. Порядок проведення такої експертизи встановлюється органом виконавчої влади за погодженням з Державною службою спеціального зв'язку та захисту інформації України. Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

ВИСНОВКИ

Інформаційно-комунікаційну діяльність, що сьогодні охоплює всі сфери життя суспільства і дозволяє швидко опрацьовувати інформацію й мати доступ до різних джерел інформації, характеризують відкритість і доступність будь-якої інформації, а заразом її незахищеність. Вдосконалення і прискорення роботи різних організацій сьогодні показує небезпеку та вразливість інформації до несанкціонованого втручання та нецільового її використання, що потребує постійного вдосконалення систем захисту інформації та діяльності у віртуальному середовищі.

Сучасний стан інформаційно-комунікаційної діяльності та техніко-технологічні можливості захисту персональних даних користувачів інформаційно-комунікаційної діяльності є достатніми та зрозуміли. Але варто враховувати що будь які системи захисту повинні проходити оновлення і вдосконалення, що суттєво підвищить безпеку інформації користувача та зробить віртуальне життя і комунікацію прозорою й захищеною.

Аналіз можливостей автоматизованої обробки інформації в системі обслуговування користувачів Районної ради Могилів-Подільська у Вінницькій області дозволив викласти основні складові роботи з даними та напрями їх подальшого використання. Виявлення проблемних складових дозволило означити шляхи вдосконалення технологій автоматизованої обробки інформації в роботі районної ради. Вивчено процедуру впровадження та використання нових систем захисту та інформаційно-комунікаційної діяльності і безпеки інформації.

Встановлено вагомість забезпечення захисту інформаційно-комунікаційної діяльності та безпеки інформації в роботі Могилів-Подільської районної ради, з метою якої постійно проводиться роз’яснювальна робота із співробітниками структурних підрозділів органів виконавчої влади та місцевого самоврядування. Надаються необхідні консультації, практичні рекомендації щодо ефективного використання технічних засобів та програмного

забезпечення, впровадження комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.

У результаті проведеного дослідження постали перспективні напрями наукового висвітлення. Актуальним є питання встановлення і забезпечення належного рівня інформаційної безпеки в роботі органів влади. Потребує спеціального вивчення питання гарантування захисту установчими і регуляторними нормативно-правовими та адміністративно-організаційними актами. Важливим питанням безпеки інформації в умовах стрімкого розвитку та застосування практично у всіх сферах життєдіяльності людини та суспільства інформаційних технологій є встановлення достатності забезпечення цілісності інформації (запобігання умисному спотворенню інформації без відома її джерела та переводу цієї інформації до категорії невірогідної; як уникнути користування «сумнівними» джерелами інформації в діяльності державних організацій).

Зрозуміло, що шлях вирішення проблем забезпечення на належному рівні інформаційної безпеки полягає у поєднанні установчих і регуляторних та адміністративно-організаційних актів із засобами, які дозволяють здійснювати протидію у «площині», у якій відбуваються дії порушення інформаційної безпеки, тобто програмних, технічних, телекомунікаційних та інших засобах та методах для забезпечення пошуку, обробки, транспортування та збереження інформації. Встановлено, що об’єктом подальших досліджень повинні стати механізми та засоби захисту самої інформації, а предметом дослідження стануть принципи, методи та засоби отримання, передачі, обробки та збереження інформації.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Закон України Про державну таємницю. № 3855-XII. 21 січня 1994 р. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

2. Закон України Про доступ до публічної інформації. № 2939-VI. 13 січня 2011 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

3. Закон України Про захист інформації в інформаційно-телекомунікаційних системах. *Відомості Верховної Ради України* (ВВР). 1994. № 31. ст.286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

4. Закон України Про інформацію. *Відомості Верховної Ради України* (ВВР). 1992. № 48. ст. 650 02 жовтня 1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

5. Закон України Про національну безпеку України. *Відомості Верховної Ради* (ВВР). 2018. № 31. ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

6. ДСТУ 2732-94. Діловодство й архівна справа. Терміни та визначення Чинний від 1994-01-01. К.: Держстандарт України, 2011. ст. 33.

7. ДСТУ 2395-94. Інформація та документація. Обстеження документа, встановлення його предмета та відбір термінів для індексування. Основні вимоги. Чинний від 1995-01-01. К.: Держстандарт України, 2019. 410 с.

8. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМУ від 8 лютого 2021 р. № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text

9. Про Доктрину інформаційної безпеки України. Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

10. Автократов В.Н., Банасюкевич В.Д., Соколова А.Н. Основные направления развития документоведения. Теоретические проблемы документоведения. Тезисы докл. и сообщ. к теор. семинару. М., 2020. С. 35-56.

11. Архивознавство: Підруч. для студ. вузів України. Я.С. Калакура (гол. ред.) та ін. К., 2019. ст. 303.

12. Байрак М.О., Боровик М.В. Діловодство й управлінська діяльність в Україні. *Уніфікована система ОРД*. 2019. № 1. 532.

13. Богуславський Г.А. Склад та види документів, що забезпечують документування управлінської інформації. *Довідник кадровика*. 2019. № 8. С. 402.

14. Бурячок В.Л Сучасне діловодство: навч. посіб. Ін-т менеджменту та економіки «Галицька академія». Центр навч. л-ри, 2018. С. 201.

15. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні: навч. посібник. К.: Юстініан, 2018. 376 с.

16. Вехов В.Б. Компьютерные преступления: Способы совершения, методики расследования. М.: Право и Закон, 2019. 281 с.

17. Горобець П.П. Документ: информационный анализ. М.: Наука 2020. 255 с.

18. Гречко А.В. Основи електронного документообігу: Навч. посібник. К., 2018. 156 с.

19. Дєгтяр О.А. Інформаційно-комунікативна діяльність в державному управлінні як інструмент інтенсифікації соціального партнерства. *Державне управління: удосконалення та розвиток*. 2013. № 9. URL: http://www.dy.nayka.com.ua/?op=1&z=623

20. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. *Наука і оборона*. 2020. № 16. С. 356-358.

21. Дрешпак В.М. Інформаційно-аналітичне забезпечення органів місцевої влади: навч. посіб. Дніпропетровськ: ДРІДУ НАДУ, 2017. 159 с.

22. Дурняк Б.В. Семантичний захист інформації в системах документообігу. Інформаційні технології. Л.: Вид-во Укр. акад. друкарства, 2017. 160 с.

23. Дубас П. Інформаційно-комунікаційний простір: поняття, сутність, структура. *Сучасна українська політика. Політики і політологи про неї*. К., 2010. Вип. 19. С. 223-232.

24. Іванова Т.В., Піддубна Л.П. Діловодство в органах державного управління та місцевого самоврядування. К.: 2007. 290 с.

25. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. К.: ДСТСЗІ СБ України, 1999. 216 с.

26. Зибін С.В. Захист інформації від несанкціонованого доступу в системах обробки інформації. *Інформаційна безпека*. 2017. № 21. 440 с.

27. Зіма І.І. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів). К.: Наука і оборона. 1998. № 1. С. 56-58.

28. Клименко І.В. Електронний документообіг у державному управлінні. К.; Х.: ФОРТ, 2018. 232 с.

29. Клименко І.В., Линьов К.О. Система електронного документообігу в державному управлінні. К.: Вид-во НАДУ, 2017. 632 с.

30. Кулешов С.Г. Документознавство: Історія. Теоретичні основи. К., 2000. 161 с.

31. Крупський С.Н. Захист інформації від несанкціонованого доступу в системах обробки інформації. К.: Наука, 2018. 256 с.

32. Круковський М.Ю. Рішення електронного документообігу. К.: Азимут-Україна. 2018. 112 с.

33. Кузьменко Б.В. Організаційно-правові та програмно-технічні засоби забезпечення інформаційної безпеки: навч. посібник. К.: НАУ, 2018. 364 с.

34. Кукарін О.Б., Логвинов В.Г., Мазуркевич М.В., Марчук О.В. Ресурс інформаційний. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2018. Т.2. Методологія державного управління. с. 545-547.

35. Кукарін О.Б., Марчук О.В. Інфраструктура електронного урядування технологічна. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2017. Т.2. Методологія державного управління. с. 235-236.

36. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2011, Т.1. Теорія державного управління. с. 518-520.

37. Кукарін О.Б., Марчук О.В. Технології інформаційні. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2018. Т.2. Методологія державного управління. с. 615-616.

38. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України. К.: Текст, 2003. 629 с.

39. Мазуркевич Т.Л., Липова С.В. Перспективи розвитку послуг е-урядування у Вінниці. *Вісник СНТ ДонНУ імені Василя Стуса.* Том 1. № 11 (2019). С. 160-165. URL: https://jvestnik-sss.donnu.edu.ua/article/view/6700

40. Мазуркевич Т.Л. Візитна картка як передумова ефективної ділової комунікації. Збірник матеріалів IV Всеукраїнської наукової конференції «Інформаційні технології і системи в документознавчій сфері». Вінниця: ДонНУ імені Василя Стуса, 2019. С. 69-70.

41. Мазуркевич Т.Л. Специфіка впровадження архіву електронних документів на підприємстві. Збірник матеріалів V Всеукраїнської наукової конференції «Інформаційні технології і системи в документознавчій сфері». Вінниця: ДонНУ імені Василя Стуса, 2020. С. 56-59.

42. Мазуркевич Т.Л. Виклики інформаційно-комунікаційної безпеки в суспільстві.. Збірник матеріалів VI Всеукраїнської наукової конференції «Інформаційні технології і системи в документознавчій сфері». Вінниця: ДонНУ імені Василя Стуса, 2021. С. 56-59.

43. Марчук О.В., Нагорна М.В., Недюха О.А., Пасічник В.М., Захист інформації. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2018. Т.2. Методологія державного управління. с. 170-172.

44. Марчук О.В. Документ електронний. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2019. Т.2. Методологія державного управління. с. 142-144.

45. Марчук О.В. Документообіг електронний. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2021. Т.2. Методологія державного управління. с. 144-146.

46. Марчук О.В. Підпис електронний цифровий. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2018. Т.2. Методологія державного управління. с. 447-449.

47. Матвієнко О.В. Основи організації електронного документообігу. К.: Центр учбової л-ри, 2008. 111 с.

48. Нестеренко О.В. Засади забезпечення необхідного рівня інформаційної безпеки державної влади: URL: http://www.nbuv.gov.ua/portal/soc_gum/nac_.pdf

49. Почепцов Г.Г., Чукут С.А. Інформаційна політика. К.: Вид-во «Знання», 2018. 665 с.

50. Рибак М.І. До питання про інформаційні війни. К.: Наука і оборона. 2018. № 2. С. 65-68.

51. Степко О.М. Аналіз головних складових безпеки держави. М.: Наука, 2018. 281 с.

52. Сорока Ю. Документознавство та його роль і місце в системі історичної науки. *Спеціальні галузі історичної науки*: Зб. на пошану Марка Якимовича Варшавчика. Редкол.: Я.С.Калакура (гол.ряд.) та ін. К., 2020. 394 с.

53. Швецова-Водка Г.М. Книга і документ в системі соціальних комунікацій. К., 2017. 564с.

54. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. К.: ДСТС31 СБ України, 1999. 26 с.

55. Про національну систему конфіденційного зв'язку України від 10 січня 2002 № 2919-III. Закон України. URL: http://www.rada.gov.ua

56. Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади. Постанова Кабінету Міністрів від 10 вересня 2003 р. № 1433. URL: https://zakon.rada.gov.ua/laws/show/1433-2003-%D0%BF#Text

57. Про затвердження Порядку обов'язкової передачі документованої інформації. Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1454: URL: http://www.rada.gov.ua

58. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова Кабінету Міністрів України від 29 березня 2006 р.№ 373: URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

59. Про затвердження загальних вимог до програмних продуктів, які закуповуються або створюються на замовлення державних органів. Постанова Кабінету Міністрів України від 12 серпня 2009 р. № 869. URL: https://zakon.rada.gov.ua/laws/show/869-2009-%D0%BF#Text

60. Про схвалення Концепції розвитку електронного урядування в Україні. Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text

61. Інформаційно-комунікаційна діяльність наукових бібліотек в умовах розвитку суспільства знань: монографія. НАН України, Нац. б-ка України ім. В.І. Вернадського. Київ, 2017. 410 с.

62. Карпенко О., Дуда А. Інформаційно-комунікативна діяльність виконавчих органів місцевих рад в Україні. Ефективність державного управління. 2017. Вип. 4 (53). Ч. 1. URL: http://www.lvivacademy.com/vidavnitstvo_1/edu_53/fail/16.pdf

63. Моісєєва Н.І. Соціально-комунікаційна діяльність як історико-суспільна практика. Монографія. Х. : ХНТУСГ, 2015. 392 с.

64. Фурашев В.М., Сутність та визначення понять «інформаційна безпека» і «безпека інформації». Правова інформатика. 2012. № 2(34). URL: http://ippi.org.ua/furashev-vm-sutnist-ta-viznachennya-ponyat-%E2%80%9Cinformatsiina-bezpeka%E2%80%9D-i-%E2%80%9Cbezpeka-informatsii%E2%80%9D

65. Архипов О., Архипова Є. Особливості розуміння понять «інформаційна безпека» та «безпека інформації». Информационные технологии и безопасность: основы обеспечения информационной безопасности (ИТБ-2014): Материалы XIV международной научно-практической конференции. К.: ИПРИ НАН Украины, 2014. С.18-30.

66. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014, № 1. URL: https://core.ac.uk/download/pdf/141443493.pdf

67. Довгань О.Д., Ткачук Т.Ю., Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. 2018. 1(24). С. 89-103. URL: http://ippi.org.ua/dovgan-od-tkachuk-tyu-sistema-informatsiinoi-bezpeki-ukraini-ontologichni-vimiri-st-89-103

ДОДАТКИ

ДОДАТОК А

Ресурси, необхідні для виконання проекту Могилів-Подільської районної ради

№	Назва роботи	Назва ресурсу	Кількість ресурсу	Виконавець	Кількість виконавців
1	Встановлення сигналізації	Датчики руку	21	Монтажники, робітники	2
2	Встановлення систем безперервного живлення	Кабель, системи живлення	4	Електрик	1
3	Встановлення захистів корпусів ПК	Кліпси, спец замки.	44	Адміністратор	1
4	Введення паролів до системи керування	-	-	Адміністратор	1
5	Перевірка паролів	-	-	Адміністратор, кожен службовець	Не визначена кіл.
6	Встановлення системи резервного копіювання Резервне копіювання І.	Система рез коп..	2	Адміністратор	1
7	Вибір антивірусного програмного забезпечення	-	-	Адміністратор	1
8	Установка антивірусного програмного забезпечення	Антивірусне ПЗ. На вибір	16	Адміністратор	1
9	Аналіз роботи всіх підрозділів та відділів, аналіз док.	-	-	Менеджер, бухгалтер, директор	8

ДОДАТОК Б

Лист УСБУ у Вінницькій області

СЛУЖБА БЕЗПЕКИ УКРАЇНИ
Управління Служби безпеки України у Вінницькій області
вул. Грушевського, 27, м. Вінниця, 21050, тел. (0432) 53-13-09
www.ssu.gov.ua, e-mail: usbu_vin@ssu.gov.ua Код ЄДРПОУ 20001473

26 04 21 № 53/30/52-2926 Ві На № _____ від _____

Ректору Донецького національного університету ім. В. Стуса
Роману ГРИНЮКУ
21021, м. Вінниця, 600-річчя, 21

Щодо загрози технічного проникнення

Шановний пане Романе!

Управлінням у ході виконання завдань із посилення захисту об'єктів критичної інфраструктури Вінницького регіону вживаються заходи з виявлення та локалізації деструктивних факторів, що можуть негативно вплинути на стан їх захищеності.

Аналіз наявної інформації свідчить про збільшення кількості випадків несанкціонованого втручання в роботу електронних інформаційних ресурсів, особливо з використанням розсилки шкідливого програмного забезпечення через електронні поштові сервіси, що може призвести до витоку інформації, що є власністю держави, й втрата якої може призвести до нанесення значної шкоди сталій діяльності державних органів.

Так, протягом 2020-2021 років на комп'ютерні системи органів влади, місцевого самоврядування, підприємств, установ та організацій здійснено спроби кібератаки шляхом направлення т. зв. «фішингових листів», які під виглядом інформації, яка могла зацікавити користувачів, у випадку переходу за посиланням могло призвести до дестабілізації діяльності електронних мереж і витоку інформації, що є власністю держави.

Довідково:

У березні поточного року з поштової скриньки lordharryloans.01@gmail.com з текстовим вмістом (Квота вашого поштової скриньки перевищила обмеження пам'яті, встановлене вашим адміністратором, і ви не зможете надсилати або отримувати нову пошту, доки не підтвердите її до натисніть тут для входу у свій обліковий запис електронної пошти для автоматичної активації) надсилався лист на адреси судової влади Вінницької області. Вказаний лист містив вкладення з шкідливим програмним забезпеченням.

Авторами подібних «листів» використовуються методи «соціальної інженерії», зокрема в результаті аналізу обставин та середовища зміст листів формується таким чином, щоб підлаштуватись під об'єкт та зацікавити користувачів з метою отримання інформації, що знаходиться в їхньому користуванні.

Ознаки фішингових листів:

1. З метою збільшення кількості відгуків на лист, зловмисники намагаються надати повідомленням екстрений характер, окреслюючи ліміт часу, і викликати необдумані дії користувача.
2. Як правило, в фішингових листах, в полі «Тема:», використовується різний регістр літер, набір літер та цифр, допускаються граматичні або друкарські помилки для уникнення фільтрів програм.
3. Посилання, зазначені в фішингових листах, ззовні схожі на офіційні веб-адреси сайтів і перенаправляють на сайти, які імітують зовнішній вигляд легітимного сайту.

Аналіз причин і умов вказаних інцидентів указує на те, що несанкціоновані втручання в роботу електронних ресурсів стали можливими завдяки ігноруванню користувачами елементарних вимог безпеки при роботі з інформацією, отриманою з мережі Інтернет, навіть у разі виявлення загрози встановленим антивірусним програмним забезпеченням. Як наслідок, створені передумови до потрапляння до локальної обчислювальної мережі установ шкідливих комп'ютерних вірусів, що, в свою чергу, може призвести до викрадення, блокування, знищення чи виток інформації.

З урахуванням викладеного, з метою недопущення несанкціонованих дій сторонніх осіб до інформації, що обробляється в ІТС навчального закладу необхідно утриматись від виконання дій, які перераховані у текстовому повідомленні, змінити пароль електронної пошти, а також забезпечити збереження слідів спроби несанкціонованого втручання шляхом копії електронного повідомлення в форматі *EML (в разі необхідності із залученням виділених фахівців УСБУ у Вінницькій області) та передачі його на нашу адресу для дослідження.

В подальшому електронний фішинговий лист підлягає видаленню.

За результатами вжиття заходів просимо письмово повідомити на нашу адресу.

З повагою

Заступник начальника Управління **Олександр ШУМАНСЬКИЙ**

Вик. Юрій ЩЕНКО
тел. 380637788177