ЗАТВЕРДЖЕНО
Наказ Вищого навчального закладу Укоопспілки
«Полтавський університет економіки і торгівлі»
18 квітня 2019 року № 88-Н

Форма № П-4.03

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД УКООПСПІЛКИ
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»

Інститут економіки, управління та інформаційних технологій
Форма навчання денна

Кафедра документознавства та інформаційної діяльності в економічних системах

Допускається до захисту
Завідувач кафедри _____Т. В. Оніпко
« 17 » грудня 2019 р.

ДИПЛОМНА РОБОТА

на тему:

«ОРГАНІЗАЦІЯ І ВДОСКОНАЛЕННЯ СИСТЕМИ БЕЗПЕКИ ДОКУМЕНТНО-ІНФОРМАЦІЙНОЇ СИСТЕМИ УСТАНОВИ»
(за матеріалами Полтавського обласного центру зайнятості)

зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
освітня програма «Документознавство та інформаційна діяльність»

Виконавець роботи Славко Ігор Олександрович

_____
(підпис, дата)

Науковий керівник д. е. н., професор Макарова Маріанна Володимирівна

_____
(підпис, дата)

Рецензент

Полтава 2019

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

ДСЗ – Державна служба зайнятості;

ЄІАС – Єдина інформаційно-аналітичної система;

ЄТОН – Єдина технологія обслуговування незайнятого населення;

ІТС – інформаційно-телекомунікаційна система;

СЗІ – система захисту інформації;

СЗУ – Служба зайнятості України;

ТЗ – технічний захист;

ТЗІ – технічний захист інформації;

ФЗДССУВБ – Фонд загальнообов'язкового державного соціального страхування України на випадок безробіття;

ЦЗ – Центр зайнятості.

ВСТУП

Документно-інформаційні системи призначені для своєчасного забезпечення та задоволення потреб користувачів в інформації. Наприклад, у діяльності установ існує практика створення та функціонування єдиної інформаційної системи, що задовольняє інформаційні потреби усіх співробітників, служб та підрозділів організації. Функціональне призначення цих систем – це забезпечення інформаційних процесів, зокрема, забезпечення створення, поширення, використання, збереження і знищення документної інформації. Такий підхід до визначення функціонального призначення інформаційних систем забезпечує інваріантність як до видів інформації й інформаційних ресурсів, так і до видів і типів інформаційних технологій, які використовуються для реалізації інформаційних процесів.

Документно-інформаційні системи є основою роботи будь-якої організації. Для забезпечення їх ефективного функціонування важливим є розробка системи захисту документно-інформаційних ресурсів. Питанням розробки і функціонування систем захисту інформації присвячено значну кількість праці Дудикевича В. Б. [32, 58], Петрова О. С. [52], Хорошка В. О. [52] та інших вчених.

Аналіз наукових публікацій дає підстави стверджувати, що у процесі проектування, створення й експлуатування систем інформаційного захисту трапляються помилки та недоречності, які суттєво знижують ефективність їх функціонування. Вимагає окремого обґрунтування розроблення політики інформаційної безпеки, яка визначає стратегію і тактику системи захисту інформації в документно-інформаційних систем підприємств та установ і враховує динаміку процесів зміни типів і рівня загроз інформації [37].

Система захисту інформації в документно-інформаційній системі установи повинна будуватися на засадах комплексності й адаптивності. Доцільно

розробляти організаційну структуру і впроваджувати систему захисту інформації в документно-інформаційні системи установ відповідно до рекомендацій міжнародних стандартів і чинного законодавства України. Такими стандартами є: ISO/IEC 27002 «Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою» ; ISO/IEC 27003 «Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації»; ISO/IEC 27004 «Інформаційні технології. Методи захисту. Вимірювання»; ISO/IEC 27005 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки»; ISO/IEC 27006 «Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою»; ISO/IEC 27011 «Інформаційні технології. Керівництво з управління інформаційною безпекою для телекомунікацій». Дотримання принципів стандартів серії ISO 27000 забезпечує керування і контроль за доступом, розробкою й обслуговуванням апаратно-програмних систем, керування безперервністю домументно-інформаційних процесів.

Документно-інформаційна система є ключовим елемент установи. Організація її захисту та забезпечення стабільності функціонування мають прямий вплив на діяльність організації. Безпека системи – це динамічне, а не статичне поняття, тому необхідним є постійний моніторинг та вдосконалення системи захисту документних та інформаційних ресурсів. Отже, питання організації та вдосконалення системи захисту інформації в документно-інформаційній системі установи є актуальною темою.

Мета і завдання роботи. Метою роботи є узагальнення питань теоретичного обґрунтування і удосконалення методичних підходів до організації та модернізації системи захисту документно-інформаційної системи установи. Постановка цієї мети дослідження зумовила необхідність вирішення у роботі таких взаємопов’язаних завдань:

– визначити теоретичні засади функціонування документно-інформаційних систем;

– дослідити основні поняття інформаційної безпеки і види загроз документно-інформаційній системі установи;

– висвітлити найпоширеніші методи захисту документно-інформаційних ресурсів установ;

– дати загальний опис діяльності Полтавського обласного центру зайнятості;

– проаналізувати Єдину технологія обслуговування незайнятого населення як основа роботи Державної служби зайнятості;

– дослідити роботу документно-інформаційної системи «Соціальні послуги та Фонд» Єдиної інформаційно-аналітичної системи державної служби зайнятості;

– визначити порядок створення комплексної системи захисту документно-інформаційних ресурсів;

– сформулювати вимоги до комплексної системи захисту Єдиної інформаційно-аналітичної системи Служби зайнятості України;

– запропонувати програму тренінгу з інформаційної безпеки як шлях реалізації політики безпеки установи.

Об’єктом дослідження є процес організації захисту документно-інформаційної системи установи.

Предметом дослідження є теоретичні засади і прикладні аспекти процесу організації і вдосконалення захисту документно-інформаційної системи установи.

Суб’єкт дослідження – Полтавський обласний центр зайнятості Державної служби зайнятості України.

Методи дослідження. Для розв’язання визначених завдань і досягнення мети кваліфікаційної випускової роботи застосовано комплекс взаємодоповнюючих загальнонаукових і спеціальних методів дослідження:

– методи систематизації і використання інформаційного матеріалу (аналіз, синтез, узагальнення, класифікації) – під час формулювання означень основних понять документно-інформаційних систем та інформаційного захисту;

– метод опитування, метод огляду документів – під час ознайомлення зі структурою та основними напрямами роботи Полтавський обласний центр зайнятості Державної служби зайнятості України;

– метод причинно-наслідкового аналізу – під час дослідження впливу загроз безпеці на діяльність установи ;

– метод порівняння – при аналізі послуг консалтингових компаній;

– графічний метод – для ілюстрації важливих аспектів і висновків дипломної роботи.

Інформаційно-методологічною базою дослідження є: законодавчі й нормативні акти; постанови Кабінету Міністрів України; наукова література; статті вітчизняних і зарубіжних учених у періодичних виданнях із питань документознавства та інформаційної діяльності; довідково-інформаційні видання; відомості мережі Інтернет; дані суб'єкта дослідження.

Наукова новизна полягає в розробці шляхів удосконалення організації системи захисту документно-інформаційної системи установи, що дозволило сформулювати загальні положення та рекомендації щодо вказаного процесу, а саме запропонована програма тренінгу з інформаційної безпеки для спеціалістів центру зайнятості.

Практична значимість результатів дослідження полягає у можливості застосування запропонованого шляху вдосконалення системи захисту в Полтавському обласному центрі зайнятості. Описаний тренінг може бути використаний у практичній діяльності установ.

За матеріалами дослідження опублікована стаття: Славко І. О. Безпека документно-інформаційної системи установи / І. О. Славко, М. В. Макарова // Збірник наукових статей магістрів. Інституту економіки, управління та інформаційних технологій. – Полтава : ПУЕТ, 2019. – Ч. 1. – С. 36-41[59].

Обсяг і структура роботи. Робота складається зі вступу, 3 розділів, 9 підрозділів, висновків, рекомендацій; містить 102 сторінки тексту, 32 рисунки, 2 таблиці, 2 додатки. Список інформаційних джерел налічує 77 найменувань літератури, у тому числі 46 електронних публікацій.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ДОКУМЕНТНО-ІНФОРМАЦІЙНОЇ СИСТЕМИ УСТАНОВИ

1.1 Теоретичні засади функціонування документно-інформаційних систем

У наш час документне середовище постійно розширюється, а документні ресурси суспільства збагачуються внаслідок впровадження новітніх інформаційних технологій, удосконалення засобів документування та розповсюдження інформації. Поняттями «інформаційні ресурси», «документні ресурси», «інформаційно-документаційні ресурси» оперують науковці та практики. Стандарт ISO (Міжнародної організації зі стандартизації) визначає «документ» як записану інформацію, яку можна розглядати як одиницю в документаційному процесі незалежно від її фізичної форми та характеристик. За Н. Литвиновою, терміни «ресурс» і «документ» в узагальнювальних значеннях, з погляду логіки, однаковою мірою застосовні до позначення різноманітних об’єктів, що розміщуються в Інтернеті [49]. Напрям розвитку термінології спрямовано в бік домінування терміна «ресурс». Вираз «документні ресурси» означає безліч конкретних ресурсів, виділених за якою-небудь ознакою: документні ресурси бібліотек, документні ресурси архівів, електронні документні ресурси.

Вказівка на «безліч» виводить на поняття «масив документів», оскільки «масив» теж припускає якусь сукупність однорідних об’єктів. На перший погляд, поняття «ресурс» можна прирівняти до поняття «масив (документів)». Між тим масив документів утворюється з його потоку, який, отже, теж є складовою документного ресурсу. Насправді документний ресурс є одночасно і масивом, і потоком документів. Документний ресурс, інакше кажучи, є набором документів і в їхній статиці, і в їхній динаміці.

Визначення «інформаційних ресурсів”, що наводяться в науковій літературі, теж підводять до думки про синонімічність цього поняття з поняттям «документні ресурси”. Наприклад: «Інформаційні ресурси – це «систематизоване зібрання науково-технічної літератури і документації, зафіксовані на паперових чи інших носіях» [14]. Поняття «документний ресурс» застосовують до окремої інформаційної системи – бібліотеки, фірми, музею, друкарні, і тоді це конкретне, часткове поняття. Від нього може бути утворено множину: «документні ресурси”.

Документні ресурси забезпечують збір, оброблення, зберігання, пошук та використання документованої інформації, тому є найважливішим видом ресурсів разом із матеріальними та енергетичними.

Документні ресурси поповнюються зовнішнім документним потоком, що виникає завдяки створенню та розповсюдженню документів. Функціонування документних комунікацій передбачає постійний рух документів комунікаційними каналами від комуніканта (створювача документної інформації) до реципієнта (споживача документної інформації). Рух документів під час їх виробництва, розповсюдження і використання у суспільстві створює документний потік.

Документний потік – це сукупність розподілених у часі і просторі документів, які рухаються комунікаційними каналами від створювачів і виробників до користувачів. Найфундаментальніше визначення документного потоку належить Г. Гордукаловій, яка визначає документальний потік як вибіркове розповсюдження у формі документів результатів соціальної діяльності членів суспільства. Під соціальною діяльністю розуміється науково-пізнавальна, управлінська, виробнича, фінансова, літературно-художня види діяльності тощо [36].

Терміни «документний» і «документальний» мають різне змістове навантаження. Лісіна С.О. зазначає, що за Столяровим Ю.М., «документний» – тобто «складається з документів”, або безпосередньо стосується документа як

фізичного об’єкта, а «документальний» означає «підтверджений документом, достовірний» [50].

Функціонування документних комунікацій у суспільстві потребує створення спеціалізованих документних систем, що забезпечують цикл життєдіяльності документів, тобто їх виробництво, транспортування, збирання, зберігання та використання. Проходячи через документні системи, документний потік створює там постійні або тимчасові сукупності документів. Тимчасові слабко-структуровані сукупності документів, що підлягають подальшому трансформуванню (відбиранню, перерозподілу та транспортуванню) – це документні масиви. Стаціонарні систематизовані, споряджені довідково-пошуковим апаратом сукупності документів, що комплектуються відповідно до завдань документної системи з обслуговування користувачів документованою інформацією – це документні фонди [50].

Фонд – це фундаментальніше утворення, ніж масив. Масив – це мобільний комплекс документів, призначений для подальшого перетворення. Фонд – це освоєний масив документів. Його освоєння відбувається за допомогою систематизації, предметизації, анотування, реферування, упорядкування за змістовими або формальними видами розташувань. Важливою ознакою фонду є його відбиття у довідково-пошуковому апараті. Документні потоки, масиви та фонди утворюють документні ресурси – сукупність документів, підготовлених для ефективного їх використання членами суспільства.

На функціонування документних ресурсів країни впливає багато факторів, головним з яких є інформативна політика держави. Вона відображається у законах і підзаконних актах, що регламентують розвиток і використання документно-комунікаційних систем країни, і спрямована на створення умов для ефективного і якісного забезпечення інформаційних потреб членів суспільства, передусім – на документне забезпечення виконання стратегічних завдань соціального та економічного розвитку держави [50].

За роки незалежності України прийнято понад двадцяти законодавчих актів щодо вдосконалення процесів формування національних документних ресурсів.

Найважливішими з них є закони України «Про інформацію» (1992 р., поточна редакція – 2019 р.), «Про друковані засоби масової інформації (пресу) в Україні» (1992 р., поточна редакція – 2018 р.), «Про науково-технічну інформацію» (1993 р., поточна редакція –2014 р.), «Про державну таємницю» (1994 р., поточна редакція – 2018 р.), «Про захист інформації в інформаційно-телекомунікаційних системах» (1994 р., поточна редакція – 2014 р.), «Про Національний архівний фонд та архівні установи» (1993 р., поточна редакція – 2015 р.), «Про бібліотеки і бібліотечну справу» (1995 р., поточна редакція – 2017 р.), «Про обов'язковий примірник документів» (1999 р., поточна редакція – 2016 р.) , «Про електронні документи та електронний документообіг» (2003 р., поточна редакція – 2018 р.), «Про захист персональних даних» (2010 р., поточна редакція – 2018 р.), «Про доступ до публічної інформації» (2011 р., поточна редакція – 2015 р.), «Про електронні довірчі послуги» (2017 р.), «Про Єдину інформаційно-аналітичну систему управління соціальною підтримкою населення України (E-SOCIAL) « (2019 р.) тощо [1-20].

На теоретичному рівні документні потоки і масиви – це складні впорядковані системи, основні компоненти яких посідають означене положення і мають певне значення. Поняття «система» – відносне, як і поняття «елемент". Наприклад, документ як система – це єдність матеріального носія та інформації, але на іншому рівні системного розгляду документ сам стає елементом загальнішої системи – документного потоку або масиву. Система утворюється тоді, коли між елементами виникають зв'язки. Вони створюють структуру системи і забезпечують її цілісність. У документних потоках і масивах як системних об'єктах зв'язки характеризуються багатоаспектністю. За напрямом розрізняють прямі і зворотні зв'язки. Документні потоки і масиви виникають під час встановлення прямих і зворотних зв'язків між створювачами і споживачами. Зовнішнє середовище, що впливає на документні потоки і масиви як систему безпосередньо або опосередковано, виявляє себе через такі основні фактори (рисунок 1.1):

– економічний – рівень і структура доходів населення країни, темпи інфляції, обсяг бюджетних асигнувань на функціонування документно-комунікаційної сфери, безробіття тощо;

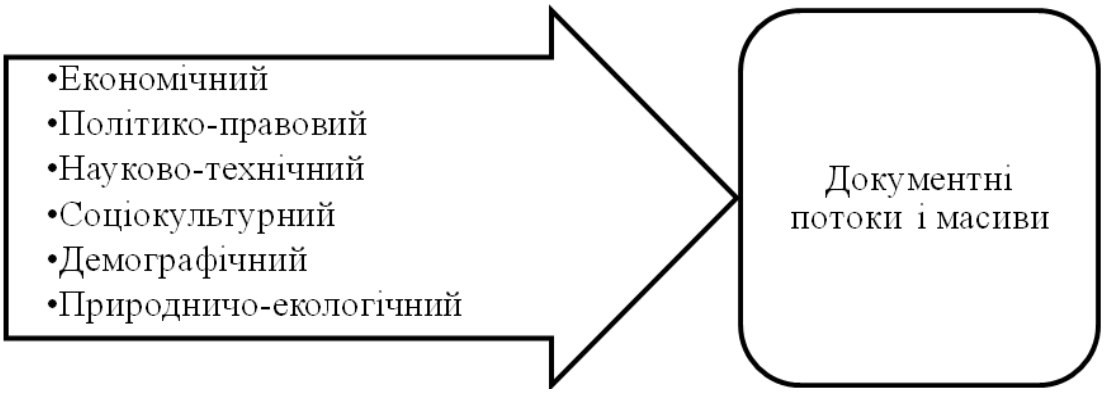

Рисунок 1.1 – Фактори впливу зовнішнього середовища на документні системи, складено автором за [50]

– політико-правовий – вплив панівного політичного режиму, офіційної ідеології, прийнятих законів та ступінь їх виконання, стан щодо дотримання прав людини;

– науково-технічний – етап у розвитку науково-технічного прогресу, технології, що використовуються, рівень комп'ютеризації тощо;

– соціокультурний – звички, традиції, панівна форма релігії, національна психологія, менталітет, грамотність населення;

– демографічний – густота населення, динаміка народження і смертності, тривалість життя, міграційні процеси тощо;

– природничо-екологічний – розміри території країни, клімат, запаси корисних копалин, особливості екологічної ситуації тощо.

Зовнішнє середовище прямого впливу – це державні органи, виробники, розповсюджувачі і користувачі документів, джерела фінансування процесів створення, розповсюдження, акумулювання документів у суспільстві. Зовнішнє середовище непрямого впливу – це рівень розвитку технологій, стан економіки, політичні і соціокультурні фактори, чинники міжнародного середовища.

Отже, системний характер документних потоків і масивів насправді мають прямі і зворотні зв'язки із зовнішнім середовищем, які безпосередньо

впливають на їх розвиток. Документно-інформаційна система потребує захисту своїх ресурсів від загроз різної природи.

1.2 Поняття інформаційної безпеки і види загроз документно-інформаційній системі установи

Інформаційна безпека – це комплексне поняття. Відповідно до законодавства України, під інформаційною безпекою розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [10].

Згідно [8] визначаються три базових рівня інформаційної безпеки, а саме: рівень особи, що передбачає формування раціонального, критичного мислення на основі принципів свободи вибору; суспільний рівень, який полягає у формуванні якісного інформаційно-аналітичного простору, багатоканальність отримання інформації, незалежні ЗМІ; державний рівень, що вміщує інформаційно-аналітичну роботу органів, інформаційне забезпечення внутрішньої та зовнішньої політики на міждержавному рівні, систему захисту інформації, протидію правопорушенням в інформаційній сфері. З огляду на це захист інформації усіх державних органів і організацій є важливою складовою загального стану безпеки, а отже, стає ще вагомішим.

Інформація – абстрактне поняття, що має різні значення залежно від контексту. На інтуїтивному рівні інформація означає зміст того, про що отримувач довідався [44] .

Інформаційна безпека є одним із найважливіших компонентів існування організації. Інформація є одним із важливих ресурсів будь-якого підприємства чи установи.

Безпека – це такі умови, у яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань і уявлень [23, 25]. Інформаційна безпека — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін «захист інформації”) [54].

Сороківська О.А. визначає інформаційну безпеку як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [59].

Інформаційна безпека характеризується конфіденційністю, цілісністю, доступністю та може розглядатися як сукупність таких елементів: безпечні умови функціонування інформаційних технологій, побудова ефективної інфраструктури інформаційного простору, цілісного ринку інформації, створення оптимальних умов для проходження інформаційних процесів.

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості тощо) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Найточніше визначення поняття «Інформаційна безпека» сформульовано в законі «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [10].

Співставлення понять безпека інформації та інформаційна безпека дозволяє дійти висновку, що друге поняття значно глибше за сутністю і ширше за змістом. Інформаційну безпеку України можна розглядати з позицій захисту не тільки інтересів держави, а насамперед особистості й суспільства. Крім цього інформаційну безпеку можна також досліджувати в контексті захисту інформаційних технологій, інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов для існування й розвитку інформаційних процесів .

Поняття інформаційної 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. Рішення про обмеження доступу приймаються на підставі спеціально розроблених переліків, наявних у кожній установі й узагальненому у Зводі відомостей, що становлять державну таємницю. Законодавчою основою подібних рішень є Закон України «Про державну таємницю» [15]. Деякі границя в захисту безпеці в ліцензійній сфері зафіксовано в Законі Україна «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв’язку та захисту інформації» [40].

У сучасних умовах перед підприємствами і організаціями гостро постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, що становлять комерційну або державну таємницю. Підприємницька діяльність тісно пов’язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Однак захисту підлягає не вся інформація, а тільки та, яка є цінною для

підприємця. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями, як корисність, своєчасність і достовірність відомостей. Розробку заходів щодо збереження комерційної таємниці підприємства слід здійснювати, дотримуючись принцип комплексного перекриття можливих каналів витоку інформації та забезпечення рівнозначної надійності захисту всіх її носіїв. Загрози збереження комерційної таємниці можуть бути зовнішніми і внутрішніми.

Дії ззовні можуть бути спрямовані на пасивні носії інформації і відбиватися, наприклад, в такому:

– спроби викрадення документів або зняття копій з документів, знімних носіїв;

– отримання інформації, що виникає на етапі передачі в процесі комунікації;

– знищення інформації або пошкодження її носіїв;

– випадкове або навмисне доведення до конкурентів документів або матеріалів, що містять комерційну таємницю.

Дії ззовні можуть бути також спрямовані на персонал організації і відбиватися у формі підкупу, погроз, шантажу, вивідування інформації, що становить комерційну таємницю, або припускати залучення провідних спеціалістів до фірми-конкурента тощо [23].

Внутрішні загрози становлять найбільшу небезпеку для знову сформованих і не усталених колективів, де не встигли скластися традиції підтримки високої репутації організації, однак увага своєчасному розкриттю цих загроз повинна приділятися повсюдно. Не виключена ймовірність того, що окремі співробітники з високим рівнем самооцінки через незадоволення своїх амбіцій, наприклад, через невдоволення рівнем заробітної плати, відносинами з керівництвом, колегами та ін., можуть вживати заходів щодо ініціативної видачі комерційної інформації конкурентам, а також спробувати знищити важливу інформацію або пасивні носії, наприклад, внести комп’ютерний вірус. За оцінками психологів, до 25% всіх службовців фірм, прагнучи заробити

кошти будь-якими способами, часто на шкоду інтересам своєї фірми очікують зручного випадку для розголошення комерційних секретів, їх продажу [23].

При оцінці загроз безпеці інформації та виборі пріоритетів у системі захисту установи проаналізуємо практику захисту інформації і забезпечення безпеки діяльності різних організацій [55].

Основним об’єктом впливу загроз безпеки є інформація, що обробляється в автоматизованих системах установи. Базисом автоматизованих систем є:

- загальносистемне програмне забезпечення;
- програмні оболонки;
- програми загального призначення;
- текстові процесори;
- редактори;
- інтегровані пакети програм.

Особливе місце в програмному забезпеченні займають системи управління базами даних. Інформація в автоматизованих системах може надходити з автоматизованого робочого місця локальної мережі внутрішніми і зовнішніми каналами зв'язку, при цьому інформація може вводитися як з клавіатури, так і з зовнішніх носіїв інформації. Крім того, автоматизована система може використовувати інформаційні ресурси інших установ і організацій і ресурси глобальних телекомунікаційних мереж [56].

До користувачів автоматизованої системи належать усі зареєстровані в ній особи або організації, наділені певними правами доступу. У рамках своїх повноважень користувач може здійснювати тільки дозволені йому дії з використанням загальносистемного і прикладного програмного забезпечення.

Процес обробки інформації в автоматизованих системах здійснюється під контролем адміністраторів системи, а її захисту – адміністраторів безпеки.

Джерела загроз безпеці інформації установи можна розділити на три групи: антропогенні, техногенні та стихійні.

У групу антропогенних джерел загроз безпеки інформації входять:

- кримінальні структури, рецидивісти і потенційні злочинці;

- недобросовісні партнери і конкуренти;
- персонал установи.

З урахуванням аналізу міжнародного досвіду захисту інформації і досвіду проведення подібних робіт у вітчизняних організаціях зловмисні дії персоналу, що працює в установі, можна розділити з урахуванням соціальних передумов на чотири основні категорії:

- переривання – припинення нормальної обробки інформації, наприклад, внаслідок руйнування обчислювальних засобів. Такі дії можуть викликати дуже серйозні наслідки, якщо навіть сама інформація при цьому не зазнає шкоди;
- крадіжка – читання або копіювання інформації, розкрадання носіїв інформації з метою отримання даних, які можуть бути використані проти інтересів власника (власників) інформації;
- модифікація інформації – внесення до даних несанкціонованих змін, спрямованих на заподіяння шкоди власнику інформації;
- руйнування даних – незворотне змінення інформації, що приводить до неможливості її використання [54].

До техногенних джерел загроз відносяться:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- засоби зв’язку, охорони, сигналізації;
- інші технічні засоби, що застосовуються в установі;
- глобальні техногенні загрози (небезпечні виробництва, мережі енерго-, водопостачання, каналізації, транспорт тощо).

До стихійних джерел загроз відносяться пожежі, землетруси, повені, урагани та інші форс-мажорні обставини. Сюди ж входять і різні непередбачені обставини і нез’ясовані явища.

Описані вище види загроз безпеці інформації систематизовано і подано на рисунку 1.2.

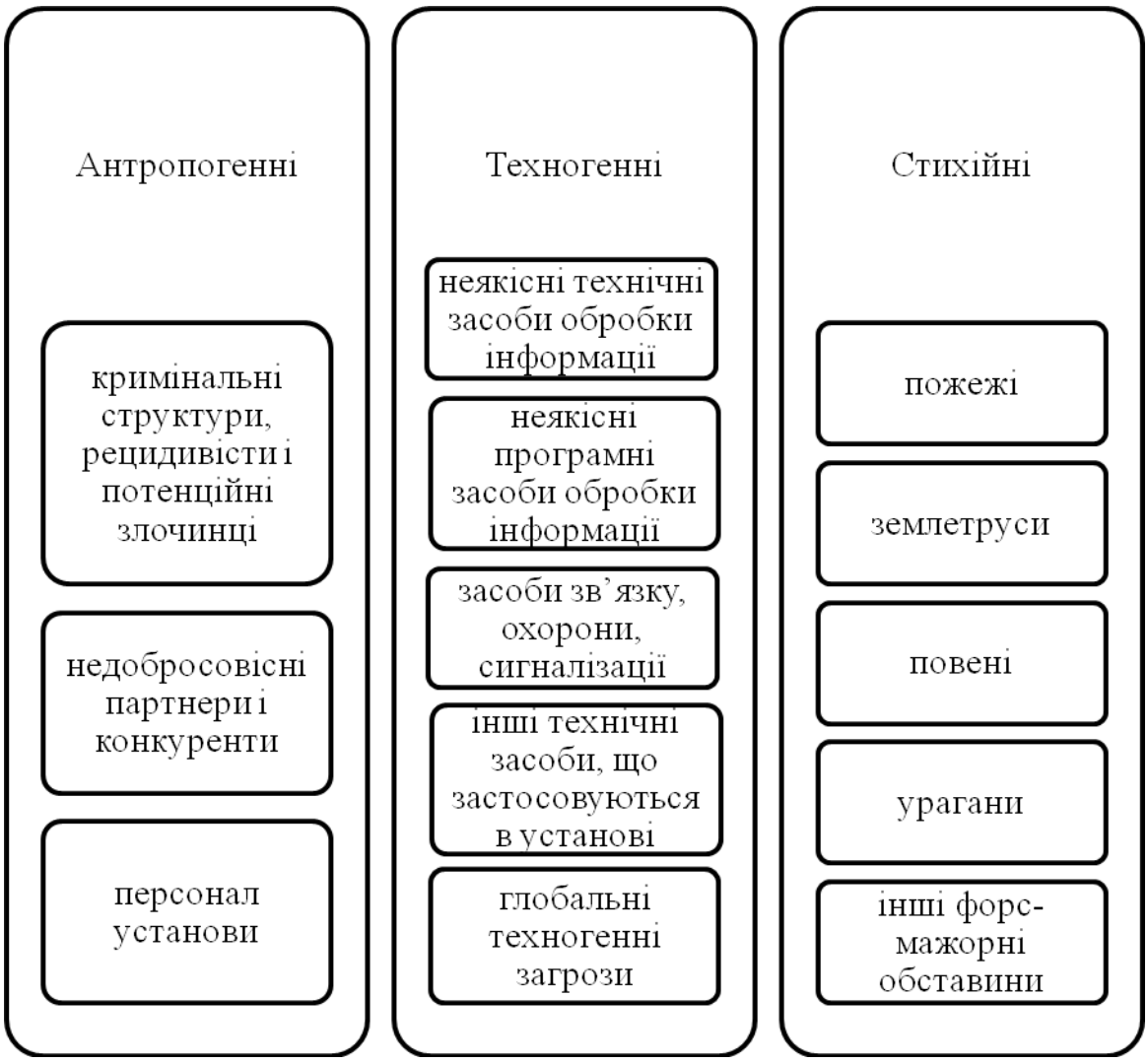

Рисунок 1.2 – Види загроз інформаційній безпеці установи, складено автором за [54]

Умовно виділяються три основних напрямки захисту інформації:

– організаційно-технічний, у межах якого створюється оболонка навколо об'єкта захисту, тобто інформаційних ресурсів, з певною мірою надійності виключає або суттєво ускладнює проведення маніпуляцій з інформацією в автоматизованій системі проти інтересів користувачів системи;

– правовий, спрямований на створення імунітету, заснованого на загрозі застосування репресивного інструменту відносно порушників інтересів користувачів системи, і встановлює механізм застосування санкцій відносно правопорушника;

– економічний, що передбачає механізм усунення матеріального збитку, завданого власнику інформації в результаті несанкціонованих дій з нею з боку правопорушника.

Організаційно-технічний напрям захисту інформації є найбільш реальним напрямом у захисті інформації підприємства. У ньому доцільно виділити два основні завдання:

– забезпечення цілісності самої інформації і процесів її обробки, передачі і зберігання;

– забезпечення конфіденційності інформації обмеженого доступу.

При аналізі завдань захисту інформації необхідно ввести деякі поняття згідно [54]:

- Обчислювальне середовище – програми і дані, що розташовуються на внутрішніх накопичувачах автоматизованих систем.

- Операційне середовище – сукупність функціонуючих в даний момент часу елементів обчислювального середовища, що знаходяться в оперативній пам'яті автоматизованої системи.

- Зовнішній компонент операційного середовища – алгоритми управління автоматизованої системи через канали зв'язку.

- Внутрішній компонент операційного середовища – елементи обчислювального середовища даної автоматизованої системи.

У [54] виділено два основні класи завдань захисту інформації:

– захист елементів обчислювального середовища – забезпечення цілісності даних, процедур обробки та конфіденційності інформації;

– контроль елементів операційного середовища – зовнішніх компонентів операційного середовища, цілісності внутрішніх компонентів обчислювальної середи і семантики даних.

Отже, існує низка загроз документно-інформаційній системі, що мають бути враховані та передбачені, тобто в установі повинні застосовуватись заходи безпеки, які допоможуть зберегти цілісність і конфіденційність даних документно-інформаційної системи.

1.3 Найпоширеніші методи захисту документно-інформаційних ресурсів установ

Проблема інформаційної безпеки вимагає комплексного вирішення, тому необхідно проаналізувати існуючі методи захисті інформаційних систем. Доктриною інформаційної безпеки України задекларовано, що життєво важливими інтересами суспільства і держави серед інших є всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної і об'єктивної інформації; забезпечення вільного обігу інформації, крім випадків, передбачених законом; розвиток і захист національної інформаційної інфраструктури тощо.

Пріоритетами державної політики щодо забезпечення інформаційної безпеки мають бути [7]:

- створення інтегрованої системи оцінки інформаційних загроз і оперативного реагування на них;
- удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави;
- визначення механізмів регулювання роботи підприємств, установ, організацій тощо.

Описані пріоритети носять глобальний характер. Для реалізації політики держави на рівні підприємств і установ використовують певні методи захисту інформації, у тому числі, документної.

Захист інформації на сьогодні є важливою темою для суспільства, а тим більше для установ будь-якого напрямку і масштабу розвитку. Метою інформаційної безпеки є збереження цілісності, повноти і точності інформації, мінімізація ризику несанкціонованих змін в інформаційних системах.

Забезпечення незмінності існуючого порядку функціонування інформаційних систем має відбуватися на трьох рівнях: адміністративному – за допомогою політики безпеки установи; локальному – шляхом формування специфічних

правил та рекомендаційних норм для персоналу; об'єктному – використання сертифікованих, легальних засобів програмного і апаратного забезпечення.

Суб’єкти впливу на документно-інформаційну систему установи поділяються на дві групи: зовнішні (злочинці, хакери, їх угрупування тощо) і внутрішні (персонал, який має доступ до інформаційних систем і технічних засобів установи).

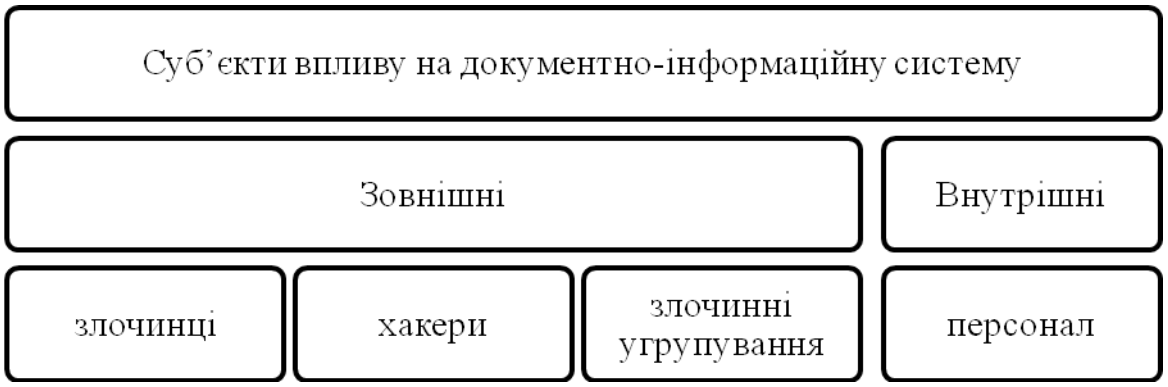

Рисунок 1.3 – Суб’єкти впливу на документно-інформаційну систему, складено автором за [25]

Аніловська Г.Я. одним із методів забезпечення інформаційної безпеки підприємства називає стандартизацію інформаційної структури інформаційної системи, елементами якої є форми існування і подання інформації у цілому, а зв’язками – операції перетворення інформації в системі. Стандартизація цього типу полягає у запровадженні єдиних правил ведення, зберігання, аналізу, оброблення інформації [23].

Одним з найефективніших методів оптимізації рівня інформаційної безпеки є конкретна програма державної політики у цій сфері, яка повинна формуватися відповідно до норм чинного законодавства.

Усі методи забезпечення інформаційної безпеки установи можна об’єднати у три групи: правові, організаційні та програмно-технічні [37].

Створення політики безпеки в інформаційній системі та інформаційній технології ґрунтується на принципі системного підходу до побудови системи захисту, що означає оптимальне поєднання взаємопов’язаних організаційних,

програмних, апаратних, фізичних та інших властивостей, підтверджених практикою створення вітчизняних і зарубіжних систем захисту і вживаних на всіх етапах технологічного циклу оброблення інформації.

Принцип безперервного розвитку системи є одним з основоположних для комп'ютерних інформаційних систем і актуальним для системи інформаційної безпеки. Інформаційні технології безперервно вдосконалюються, тому гарантування безпеки документно-інформаційної системи не може бути одноразовим актом. Це безперервний процес, що наведено в рисунку 1.4.

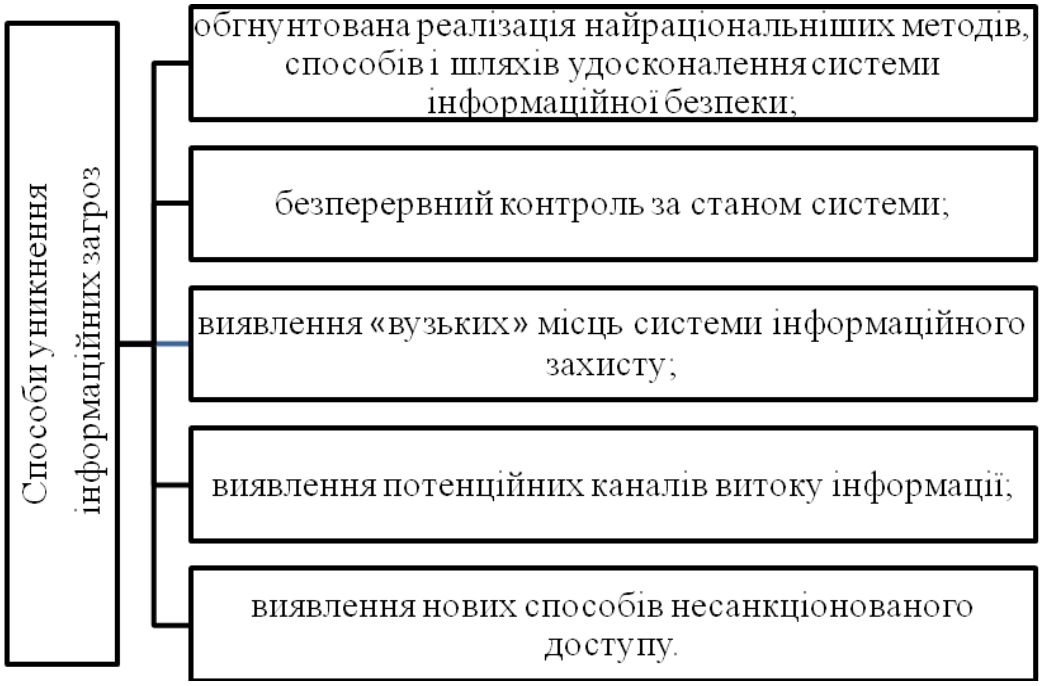

Рисунок 1.4 – Способи уникнення інформаційних загрози, складено автором за [37]

Є декілька загальновживаних заходів підтримки належного рівня захищеності системи. Серед них – розмежування і мінімізація прав доступу до оброблюваної інформації і процедур обробки, тобто надання як користувачам, так і працівникам інформаційної системи мінімуму певних повноважень, достатніх для виконання ними своїх службових обов'язків.

Повнота контролю і реєстрації спроб несанкціонованого доступу означає необхідність точно встановлювати ідентичність кожного користувача і

протоколювання його дій для проведення можливого розслідування, а також неможливість здійснювати будь-яку операцію з оброблення і інформації без її попередньої реєстрації.

Забезпечення надійності системи захисту полягає в неможливості зниження рівня надійності у разі виникнення у системі збоїв, відмов, навмисних дій зломлювача або ненавмисних помилок користувачів і обслуговуючого персоналу [23]. Забезпечення контролю за функціонуванням системи захисту – це створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення економічної доцільності використання системи захисту, що полягає в перевищенні можливого збитку інформаційних систем і технологій від реалізації загроз над вартістю розроблення й експлуатації системи інформаційної безпеки [53].

Система інформаційної безпеки має певні види забезпечення (рисунок 1.5), спираючись на які вона здатна виконувати свою цільову функцію.

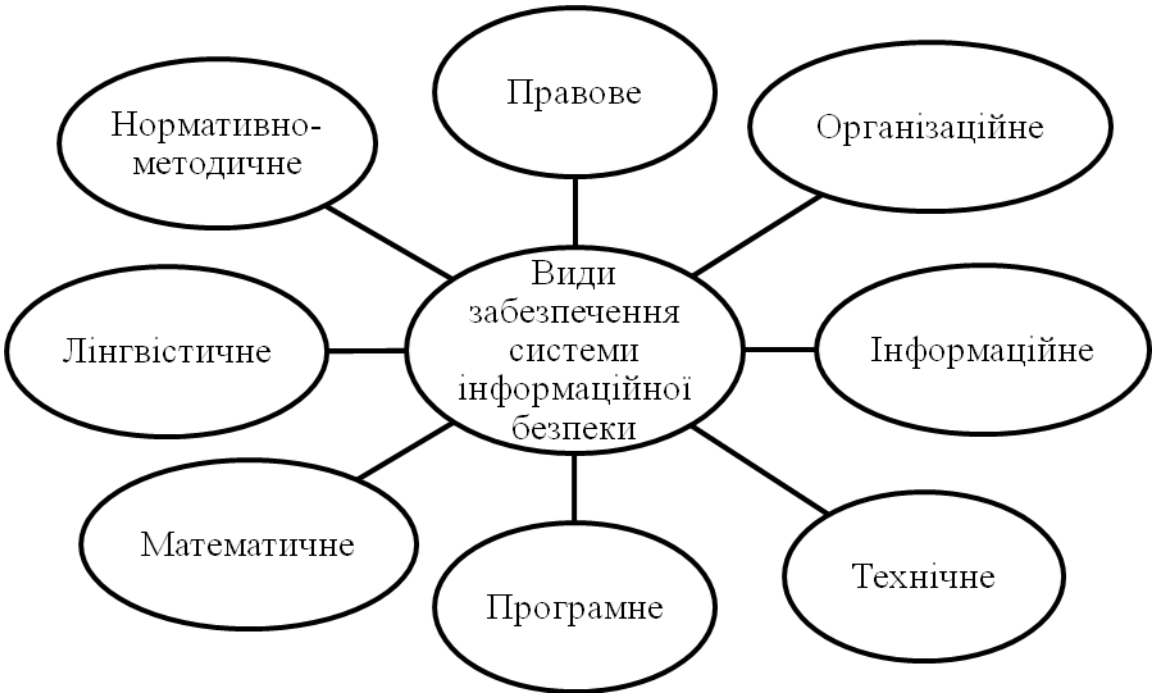

Рисунок 1.5 – Види забезпечення системи інформаційної безпеки, складено автором за [53]

Розглянемо подані на рисунку 1.5 види забезпечення детальніше. Правове забезпечення – це сукупність законодавчих актів, нормативно-правових

документів, положень, інструкцій, вимоги яких є обов'язковими у межах сфери їх діяльності в системі захисту інформації. Організаційне забезпечення – це гарантування інформаційної безпеки певними структурними одиницями. Інформаційне – це відомості, показники, параметри, що є підставою для вирішення завдань, які забезпечують функціонування системи інформаційної безпеки (показники доступу, обліку, зберігання, різні розрахункові завдання, пов'язані з діяльністю служби безпеки).

Технічне (апаратне) забезпечення передбачає широке використання технічних засобів для захисту інформації та забезпечення діяльності системи інформаційної безпеки. Програмне забезпечення – це різні інформаційні, облікові, статистичні й розрахункові програми, що забезпечують оцінювання наявності й небезпеки різних каналів витоку інформації та способів несанкціонованого доступу до неї. Математичне забезпечення – це математичні методи, які використовують для різних розрахунків, пов'язаних з оцінюванням небезпеки технічних засобів, які мають зловмисники, сфер і норм необхідного захисту. Лінгвістичне забезпечення – це сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері гарантування інформаційної безпеки.

Нормативно-методичне забезпечення, що є дотичним з правовим, містить: норми і регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації; різні методики, що забезпечують діяльність користувачів при виконанні своєї роботи за жорстких вимог дотримання конфіденційності.

Нині провідну роль відіграють організаційні заходи захисту інформації. Тому виникає питання щодо організації служби безпеки. Реалізація політики безпеки потребує налаштування засобів захисту, управління системою захисту і здійснення контролю функціонування інформаційної системи. Завдання управління і контролю зазвичай вирішуються адміністративною групою, склад і розмір якої залежать від певних умов. Часто така група працює у складі: адміністратор безпеки, менеджер безпеки і оператори.

В Інтернеті, найбільшій мережі світу, атаки на комп'ютерні системи особливо актуальні, вони не знають державних кордонів, не враховують расових чи соціальних відмінностей. Відбувається постійна боротьба інтелекту, а також організованості системних адміністраторів і винахідливості хакерів [53].

Для запобігання загрозам інформаційній безпеці та їх усунення використовують правові, програмно-технічні й організаційно-економічні методи (рисунок 1.6).

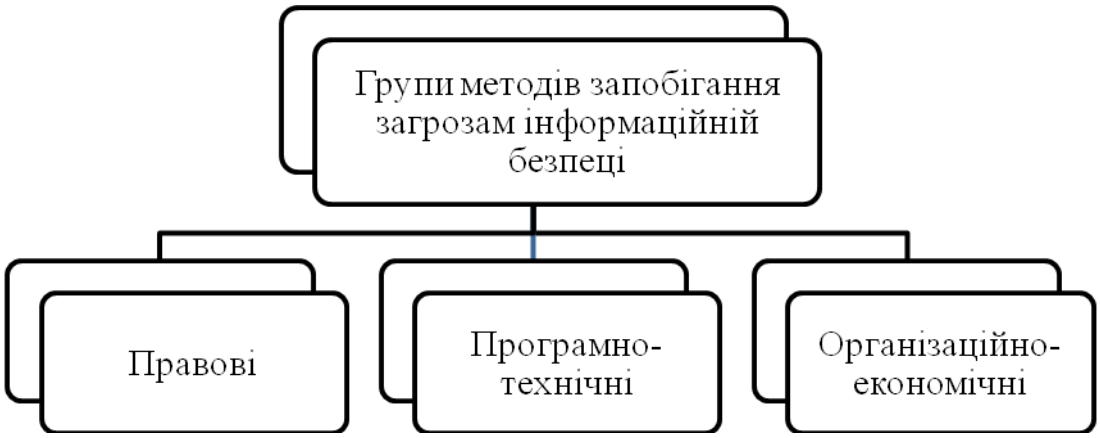

Рисунок 1.6 – Групи методів запобігання загрозам інформаційній безпеці, складено автором за [53]

Правові методи передбачають розроблення комплексу нормативно-правових актів і положень, що регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо гарантування інформаційної безпеки.

Програмно-технічні методи – це сукупність засобів:

- запобігання витоку інформації;
- усунення можливості несанкціонованого доступу до інформації;
- запобігання впливу, які призводять до знищення, руйнування, переключення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації;
- виявлення вмонтованих пристроїв;
- запобігання перехопленню інформації технічними засобами;

– використання криптографічних засобів захисту інформації під час передачі каналами зв’язку [53].

Організаційно-економічні методи передбачають:

– формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації;

– сертифікацію цих систем відповідно до вимог інформаційної безпеки;

– ліцензування діяльності у сфері інформаційної безпеки;

– стандартизацію способів і засобів захисту інформації;

– контроль за діями персоналу в захищених інформаційних системах.

Важливими для запобігання інформаційним загрозам є мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу, який забезпечує інформаційну безпеку.

Управління доступом – це методи захисту інформації регулюванням всіх ресурсів інформаційної системи та інформаційних технологій. Ці методи протистоять можливим способам несанкціонованого доступу до інформації.

Управління доступом виконує такі функції захисту:

– ідентифікацію користувачів, персоналу й ресурсів системи (закріплення за кожним об’єктом персонального ідентифікатора);

– впізнавання (визначення достовірності) об’єкта або суб’єкта за пред’явленим ним ідентифікатором;

– перевірка повноважень (перевірка відповідності дня тижня, часу доби запрошуваних ресурсів і процедур у межах встановленого регламенту);

– дозвіл і створення умов роботи в межах встановленого регламенту;

– реєстрація звернень до конфіденційних ресурсів;

– реагування (сигналізація, відключення, затримка робіт, відмова в запиті) у разі спроб несанкціонованих дій.

Механізми шифрування – криптографічне закриття інформації. Цей метод захисту дедалі ширше застосовується під час опрацювання та при зберіганні інформації на різних носіях. У разі передавання інформації каналами зв’язку великої протяжності цей метод є надійним [53].

Протидія атакам шкідливих програм припускає комплекс різних організаційних заходів і використання антивірусних програм. Мета протидії атакам:

- зменшення вірогідності інфікування інформаційної системи;
- виявлення фактів зараження системи;
- зменшення наслідків інформаційних інфекцій;
- локалізація або знищення вірусів;
- відновлення пошкодженої інформації в інформаційній системі.

Регламентація – це створення таких умов автоматизованого опрацювання, зберігання і передавання інформації, що підлягає захисту, за яких норми і стандарти захисту найбільш ефективні.

Примушення – це метод захисту, за якого користувачі і персонал інформаційної системи змушені дотримуватися правил опрацювання, передавання і використання конфіденційної інформації через загрозу матеріальної, адміністративної і кримінальної відповідальності.

Спонукання – метод захисту, що спонукає користувачів і персонал інформаційної системи не порушувати встановлених порядків за рахунок дотримання моральних і етичних норм, що склалися.

Усю сукупність технічних засобів поділяють на апаратні й фізичні. Крім того є програмні та організаційні, правові й морально-етичні засоби.

Апаратні засоби – це пристрої, які вбудовують безпосередньо в обчислювальну техніку. Фізичні засоби – це різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об’єкти захисту і здійснюють захист персоналу (особисті засоби безпеки), матеріальних засобів і фінансів, інформації від протиправних дій (замки на дверях, решітки на вікнах, засоби електронної охоронної сигналізації). Програмні засоби – спеціальні програми і програмні комплекси, призначені для захисту інформації в інформаційній системі.

Із засобів програмного забезпечення системи захисту варто виділити ще програмні засоби, що реалізують механізми шифрування (криптографії).

Організаційні засоби здійснюють регламентацію виробничої діяльності в інформаційній системі і взаємовідносин виконавців на нормативно-правовій основі так, що розголошення, витік і несанкціонований доступ до конфіденційної інформації стають неможливими або досить складними за рахунок проведення організаційних заходів. Комплекс цих заходів реалізує група інформаційної безпеки, але має бути під контролем першого керівника.

Законодавчі засоби захисту визначаються законодавчими актами країн, якими регламентуються правила користування, опрацювання і передавання інформації обмеженого доступу і встановлюють заходи відповідальності за порушення цих правил [53].

Морально-етичні засоби захисту – це різні норми поведінки, які традиційно склалися раніше, формуються у спосіб розповсюдження інформаційних систем та інформаційних технологій в країні і світі або спеціально розробляються. Вони можуть бути неписані (чесність) або оформлені в якесь зведення правил чи розпоряджень (статут). Ці норми зазвичай не є законодавчо затвердженими, але оскільки їх недотримання призводить до падіння престижу організації, вони вважаються обов’язковими для виконання.

Інформація є цінним ресурсом. Існує багато методів негласного зняття інформації:

- прослуховування телефонних ліній;
- акустичний контроль приміщення;
- прихована фото- та відеозйомка;
- перехоплення комп’ютерної інформації;
- візуальний нагляд;
- підкуп працівників;
- підкуп родичів працівників;
- приймання паразитних електромагнітних випромінювань.

Акустичний контроль приміщення можливий за допомогою: мікрофона, з виведенням сигналу кабелем; диктофона; стетоскопа; радіомікрофона; телефонної лінії.

Спеціальні мікрофони мають дуже маленькі розміри. Інформація із мікрофона передається кабелем до сусідньої кімнати, де виконується її запис. Вузькоспрямований мікрофон дає змогу прослуховувати на відстані до кілометра [53].

Професійні цифрові диктофони, незважаючи на маленькі розміри, дають змогу безперервно записувати до двадцяти годин розмов. Якщо використати функцію акустопуску (запис здійснюється лише тоді, коли хтось говорить), то залишений диктофон може записувати інформацію дуже довго. Останнім часом диктофони вмонтовують у предмети побуту.

Стетоскоп – прилад, що дає можливість прослуховувати крізь товсті стіни (до 1 м). Радіомікрофон – основний пристрій для негласного отримання інформації. Залишений один раз в офісі «жучок» буде роками передавати акустичну інформацію радіоканалам. Розміри цих «жучків» залежать від розміру блоку живлення. Якщо «жучок» живиться від стороннього джерела (наприклад, від телефонної лінії), то він зовсім непомітний [53].

Телефонну лінію використовують не лише для прослуховування телефонних розмов, а й для прослуховування офісу (при цьому трубка лежить на телефонному апараті). Для цього використовують мікрофонний ефект, високочастотне нав’язування, системи «телемонітор», «телефонне вухо» та ін. Деякі системи дають змогу прослуховувати будь-яке приміщення, через котре проходить телефонний кабель, навіть з іншої держави. За допомогою спеціального лазера можна прослуховувати офіс через зачинене вікно з відстані до кілометра.

Розвиток нових інформаційних технологій і загальна комп’ютеризація зробили інформаційну безпеку обов'язковою і однією з характеристик інформаційної системи. Існує досить розповсюджений клас систем опрацювання інформації, при розробленні яких чинник безпеки відіграє першочергову роль, зокрема банківські інформаційні системи.

Безпека інформаційної системи – це захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб

розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її компонентів. Тобто це здатність протидіяти різним протизаконним діям на інформаційну систему.

Загроза безпеці інформації – події або дії, які можуть призвести до спотворення, несанкціонованого використання чи руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Одержати інформацію з комп'ютера можна за допомогою: «хакерського» мистецтва; прихованої камери; спеціального радіоприймача, який приймає паразитичні випромінювання комп'ютера (як правило – монітора) із наступним детектуванням корисної інформації.

Багато хто вважає, що в рівній гладенькій стіні кімнати з євроремонтом неможливо сховати відеокамеру так, щоб її ніхто не побачив. Насправді це можливо [53]. Будь-яка побутова техніка має побічні електромагнітні випромінювання, які можуть бути про модульовані акустичним сигналом (голосом людини).

Існує безліч методів боротьби із несанкціонованим зняттям інформації. Але найважче боротися із новими, нестандартними методами зняття інформації. Зокрема, дуже важко звичайними методами знайти напівактивний мікрофон, котрий працює через резонатор з вібратором, без джерела живлення, що налаштований на частоту зовнішнього джерела електромагнітного випромінювання (наприклад, паразитне випромінювання розташованого недалеко заводу). Під дією зовнішнього поля в резонаторі виникає електрорушійна сила, що є джерелом випромінювання вібратора. Останній під дією акустичного сигналу коливається, тим самим модулюючі випромінювання сигнал. Складність виявлення радіомікрофона полягає в тому, що для цього потрібне зовнішнє випромінювання з частотою резонатора. Адже цей радіомікрофон може бути виконаний у вигляді звичайної побутової речі, котра не має жодного радіоелемента.

Карту зайнятості радіоефіру складають як у разі ввімкнених, так і вимкнутих електроприладів, як за опущеної, так і за піднятої телефонної трубки.

Для захисту інформації можна встановити спеціальне обладнання, подане на рисунку 1.7.

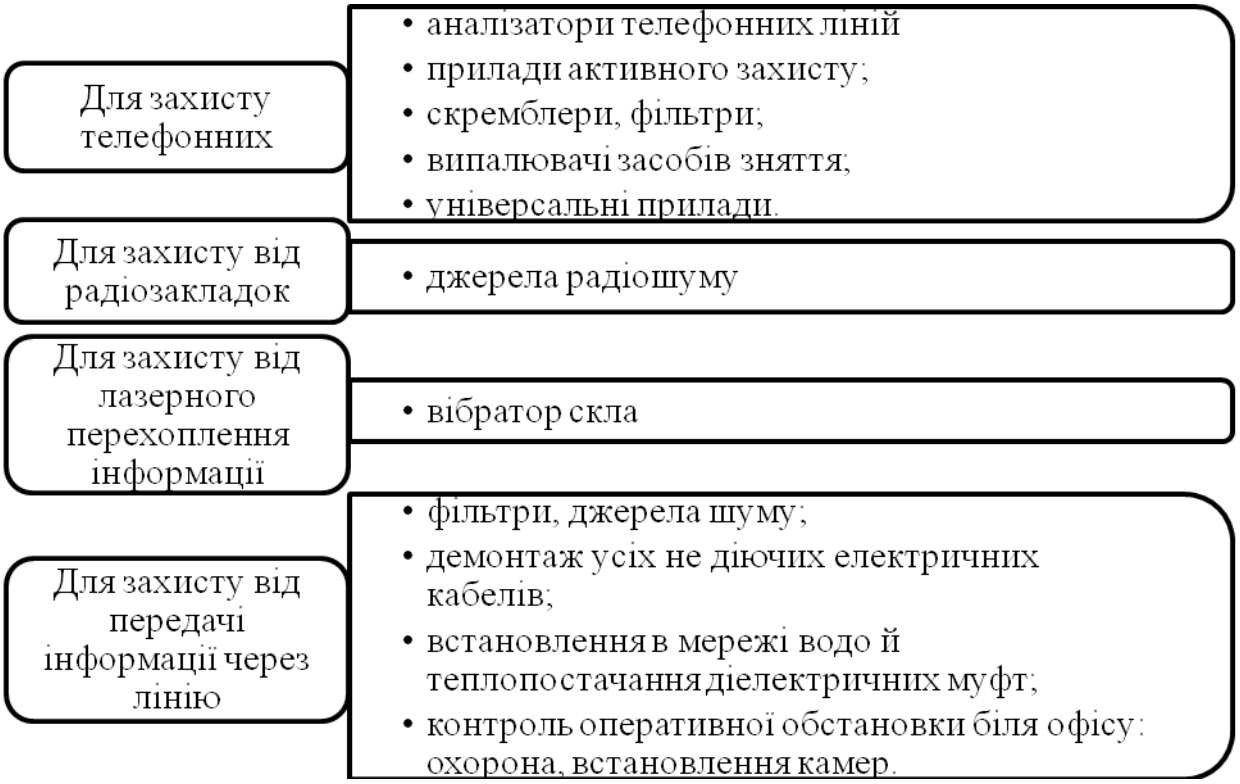

Рисунок 1.7 – Обладнання для захисту інформації,
складено автором за [53]

Тобто засобів та методів забезпечення безпеки інформації багато, та кожен з них застосовуються до певного виду інформації та структури її подання й отримання. Найважливішим є те, що потрібно будь-яким способом забезпечити безпеку документно-інформаційної системи задля збереження її цілісності [53].

Описані вище методи та засоби захисту інформації дозволяють зробити висновок про необхідність для кожної установи мати систему захисту своїх документних та інформаційних ресурсів, тобто утворення певного комплексу, який охоплює усі аспекти безпеки документно-інформаційної системи.

РОЗДІЛ 2 АНАЛІЗ СТАНУ ДОКУМЕНТНО-ІНФОРМАЦІЙНОЇ СИСТЕМИ ПОЛТАВСЬКОГО ОБЛАСНОГО ЦЕНТРУ ЗАЙНЯТОСТІ

2.1 Загальна характеристика діяльності Полтавського обласного центру зайнятості

Полтавський обласний центр зайнятості – це структурний підрозділ Державної служби зайнятості(СЗ), яка є централізованою системою державних установ, діяльність якої спрямовується та координується Міністерством соціальної політики України.

Державна служба зайнятості створена в грудні 1990 року на підставі постанови Кабінету Міністрів Української РСР від 21.12.1990 № 381 «Про створення державної служби зайнятості в Українській РСР» [11] шляхом перебудови діючої на той час служби працевлаштування на спеціалізовану службу, до завдань якої належить забезпечення комплексного вирішення питань, пов'язаних з регулюванням зайнятості населення, професійною орієнтацією, працевлаштуванням, соціальною підтримкою тимчасово непрацюючих громадян.

Основним законодавчим актом, який регулює діяльність державної служби зайнятості, став Закон України «Про зайнятість населення» [13] (№ 803-XII від 01.03.1991). Цей закон визначив соціальні гарантії з боку держави в реалізації громадянами права на працю та основні засади діяльності державної служби зайнятості.

З 1 січня 2001 року у зв’язку з набранням чинності Закону України «Про загальнообов'язкове державне соціальне страхування на випадок безробіття» [6] (№ 1533-III від 02.03.2000) та створенням Фонду загальнообов'язкового державного соціального страхування України на випадок безробіття функції

виконавчої дирекції Фонду покладені на державну службу зайнятості. Управління Фондом здійснюється на паритетній основі представниками державної сторони, застрахованих осіб та роботодавців.

На сьогодні Полтавський обласний центр зайнятості є активним посередником на ринку праці між роботодавцями і шукачами роботи, вона на безоплатній основі надає послуги із пошуку підходящої роботи та підбору персоналу, послуги з державного соціального страхування на випадок безробіття, а також здійснює виплату матеріального забезпечення у зв'язку з тимчасовою втратою роботи.

Головні завданнями державної служби зайнятості на сучасному етапі подані на рисунку 2.1.

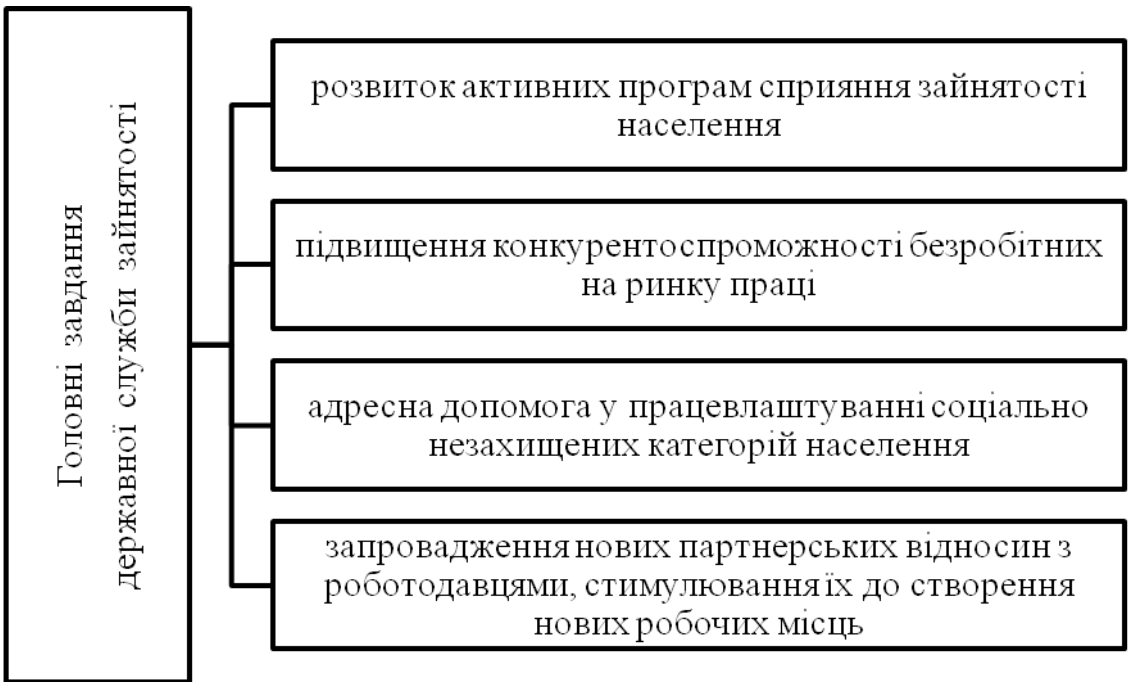

Рисунок 2.1 – Головні завдання державної служби зайнятості, складено автором за [39]

Сьогодні Державна служба зайнятості – це структура, яка об’єднує 25 регіональних центрів зайнятості, 95 базових та 429 філій регіональних центрів зайнятості (далі – ЦЗ) всією Україною, у тому числі й Полтавський обласний

центр зайнятості [39]. Усі регіональні центри є уніфікованими, що дозволяє розробити єдині правила та стандарти їх функціонування. Структура державного центру зайнятості подана на рисунку 2.2.

Рисунок 2.2 – Структура Державного центу зайнятості, скриншот [39]

Полтавський обласний центр зайнятості очолюється директором, якому підпорядковуються відділи, причому він має двох заступників, чиї повноваження розділено на фінансову та управлінську складові. Безпосередньо

директору підпорядковуються департамент реалізації політики зайнятості, основними завданнями якого є надання послуг населенню та роботодавцям. Управління надання послуг населенню має три відділи, що займаються питаннями працевлаштування, реєстрації та виплати допомоги по безробіттю, а також надання професійних та консультаційних послуг. Саме із представниками цього управління мають справу громадяни, які звертаються до державної служб зайнятості. Наданням послуг роботодавцям і безпосередньою реалізацією активних програм зайнятості займається відповідне управління.

Якщо розглядати роботу Полтавського обласного центру зайнятості з ракурсу його роботи з громадянами і роботодавцями, то департамент реалізації політики зайнятості є ключовою ланкою цієї установи. Проте її робота неможлива без усіх інших відділів. Зокрема, юридичне управління має на меті забезпечення відповідності роботи установи нормативно-правовим.

Усі відділення Полтавської обласної служби працюють за єдиною схемою надання послуг. Клієнти можуть звернутися до будь-якого центру зайнятості та отримати всі передбачені законодавством соціальні послуги, пов’язані з працевлаштуванням. У службі зайнятості створена уніфікована оперативна база вакансій, пошукачів роботи і можливостей проходження професійного навчання усією країною. Це дозволяє розширити зону пошуку роботи для безробітних не тільки в межах району чи області, а й держави в цілому.

Служба зайнятості постійно модернізується та розвивається, дбає про постійне вдосконалення соціального захисту українських громадян від безробіття.

Державна служба зайнятості є центральним апаратом Фонду загальнообов’язкового державного соціального страхування України на випадок безробіття. Відповідно до статті 10 Закону України «Про загальнообов’язкове державне соціальне страхування на випадок безробіття» [6] управління Фондом здійснюється на паритетній основі державою, представниками застрахованих осіб і роботодавців.

Правління Фонду, що створено відповідно до Закону [6], розпочало свою діяльність у межах повноважень, починаючи з першого засідання правління Фонду – 6 липня 2000 року, відповідно до постанови Кабінету Міністрів України від 14 червня 2000 року № 955 «Про організаційні заходи щодо запровадження загальнообов'язкового державного соціального страхування на випадок безробіття» [21].

Організаційну роботу щодо формування першого складу правління Фонду, а також проведення його першого засідання здійснив у 2000 році Український координаційний комітет сприяння зайнятості населення відповідно до прикінцевих положень Закону. З метою забезпечення впровадження з 1 січня 2001 року положень Закону діяльність правління Фонду протягом 2000 року спрямовувалась на вжиття організаційних заходів та заходів щодо розробки підзаконних актів, формування реєстру платників внесків на загальнообов'язкове державне соціальне страхування на випадок безробіття, вдосконалення системи контролю за повнотою та своєчасністю сплати внесків, забезпечення адаптації інформаційно-довідкової автоматизованої системи державної служби зайнятості. Так, правлінням Фонду розроблено та затверджено Статут Фонду, Регламент роботи правління Фонду.

До складу правління Фонду входять по п'ять представників від держави, застрахованих осіб та роботодавців, які виконують свої обов'язки на громадських засадах. Представники держави призначаються Кабінетом Міністрів України. Представники застрахованих осіб і роботодавців обираються (делегуються) репрезентативними на національному рівні всеукраїнськими об'єднаннями профспілок і всеукраїнськими об'єднаннями організацій роботодавців. Порядок обрання (делегування) таких представників визначається сторонами соціального діалогу самостійно [39]. Строк повноважень членів правління Фонду становить шість років і закінчується в день першого засідання нового складу правління Фонду. Правління Фонду очолює голова, який обирається з членів правління Фонду строком на два роки

почергово від представників кожної сторони. Голова правління Фонду має двох заступників, які разом з головою представляють сторони.

Відповідно до статті 11 Закону [6] правління Фонду визначає перспективні і поточні завдання Фонду; обирає голову правління Фонду і його заступників; затверджує статут Фонду; схвалює проект річного бюджету фонду і подає в установленому порядку Міністерству соціальної політики України для внесення на затвердження Кабінету Міністрів України; заслуховує звіт про виконання бюджету Фонду; вносить центральному органу виконавчої влади у сфері соціальної політики пропозиції щодо розміру частини єдиного внеску на загальнообов'язкове державне соціальне страхування, що спрямовується на страхування на випадок безробіття; вирішує інші питання відповідно до статуту Фонду.

Серед найважливіших питань, що перебувають на постійному контролі правління Фонду, є формування і виконання бюджету Фонду, визначення основних пріоритетних завдань Фонду, вдосконалення нормативно-правової бази, що регламентує внутрішню діяльність Фонду та інші рішення, зокрема щодо підвищення ефективності діяльності Фонду. За роки існування правління Фонду створено дієву систему соціального партнерства і надійну систему соціального захисту населення від безробіття на страхових засадах.

Відповідно до статті 7 Закону України «Про загальнообов'язкове державне соціальне страхування на випадок безробіття» [10] видами соціальних послуг за цим Законом і Законом України «Про зайнятість населення» [11] є:

- професійна підготовка або перепідготовка, підвищення кваліфікації у професійно-технічних і вищих навчальних закладах, у тому числі в навчальних закладах державної служби зайнятості, на підприємствах, в установах, організаціях;
- профорієнтація;
- пошук підходящої роботи і сприяння у працевлаштуванні, у тому числі, шляхом організації громадських та інших робіт тимчасового характеру у порядку, встановленому Кабінетом Міністрів України;

– надання роботодавцям, які працевлаштовують громадян, зазначених у частині першій статті 14 Закону України «Про зайнятість населення», компенсації відповідно до статті 26 Закону України «Про зайнятість населення» [11];

– надання роботодавцям – суб'єктам малого підприємництва, які працевлаштовують безробітних, компенсації відповідно до статті 27 Закону України «Про зайнятість населення» [11];

– надання ваучера для підтримання конкурентоспроможності деяких категорій громадян шляхом перепідготовки, спеціалізації, підвищення кваліфікації за професіями і спеціальностями для пріоритетних різновидів економічної діяльності відповідно до статті 30 Закону України «Про зайнятість населення» [11];

– здійснення заходів сприяння зайнятості внутрішньо переміщених осіб відповідно до статті 24-1 Закону України «Про зайнятість населення» [11];

– інформаційні й консультаційні послуги, пов'язані з працевлаштуванням.

За Законом України «Про загальнообов’язкове державне соціальне страхування на випадок безробіття» видами забезпечення є: допомога по безробіттю, у тому числі одноразова її виплата для організації безробітним підприємницької діяльності; допомога на поховання у разі смерті безробітного або особи, яка перебувала на його утриманні.

Послуги громадянам та роботодавцям надаються державною службою зайнятості безкоштовно. Консультацію щодо надання послуг ви можете отримати в будь-якому центрі зайнятості.

Центри зайнятості надають послуги з профорієнтації. Професійна орієнтація осіб, які звернулися до державної служби зайнятості, здійснюється шляхом професійного інформування, професійного консультування і професійного відбору. Будь-який громадянин, який відвідав центр зайнятості, може отримати інформацію про сучасний світ професій, їх зміст і вимоги до працівника, стан і перспективи розвитку ринку праці, підприємства і актуальні вакансії, послуги служби зайнятості щодо сприяння працевлаштуванню.

Інформування у межах профорієнтації забезпечується шляхом вільного доступу громадян до джерел інформації, надання індивідуальних інформаційних консультацій, залучення до участі у інформаційних заходах центру зайнятості.

Професійне консультування здійснюється з метою допомоги у виборі або зміні професії, виду діяльності з урахуванням індивідуально-психологічних характеристик, професійних інтересів, нахилів, стану здоров'я, особливостей життєвих ситуацій і потреби ринку праці. Індивідуальна профконсультація проводиться для осіб, які не мають професії, або для осіб, які бажають змінити професію. За згодою особи послуги з профконсультування можуть супроводжуватися психодіагностичиним тестуванням. Також, профконсультування передбачає проведення центрами зайнятості заходів щодо оволодіння громадянами навичками пошуку вакансій, складання резюме (відео-резюме), проведення співбесід з роботодавцем тощо.

Отримати послуги з професійного консультування можна за рекомендаціями фахівців центру зайнятості або за власним бажанням.

Професійний відбір проводиться:

- для відбору безробітних на профнавчання під замовлення роботодавця;
- для відбору претендентів на вакантні посади на замовлення роботодавця.

Послуги з професійного відбору супроводжуються психодіагностичним тестуванням. Особи мають можливість взяти участь в професійному відборі за рекомендаціями фахівців центру зайнятості та за власним бажанням.

Полтавський обласний центр зайнятості співпрацює також з роботодавцями. Види послуг, які надає роботодавцям державна служба зайнятості:

1. Інформування про стан, основні тенденції і процеси на локальному ринку праці.

2. Інформування роботодавців відповідно до профілю підприємств про професійно-кваліфікаційний склад осіб, які зареєстровані в центрі зайнятості, в тому числі про осіб, які шукають роботу і мають унікальні (рідкісні) професії, спеціальності або особисті якості.

3. Вивчення потреб роботодавця і надання допомоги щодо укомплектування підприємств персоналом.

4. Здійснення на замовлення роботодавця підбору необхідних працівників із використанням психодіагностичних методик: проведення тестування, оцінка та інтерпретація результатів.

5. Задоволення потреб роботодавців у тимчасових працівниках для виконання громадських та інших робіт тимчасового характеру.

6. Допомога в оперативному підборі необхідних кадрів шляхом представлення вакансій для потенційних працівників під час проведення ярмарок вакансій.

7. Організація підготовки, перепідготовки і підвищення кваліфікації безробітних з урахуванням поточної і перспективної потреби роботодавців у навчальних закладах, так і безпосередньо на виробництві.

8. Стимулювання діяльності роботодавців, спрямованої на створення нових робочих місць шляхом щомісячної компенсації єдиного внеску на загальнообов'язкове державне соціальне страхування.

9. Надання роботодавцям компенсації витрат на оплату праці працевлаштованих осіб з числа внутрішньо переміщених осіб і компенсації витрат роботодавця, який працевлаштовує зареєстрованих безробітних з числа внутрішньо переміщених осіб, на перепідготовку і підвищення кваліфікації.

10. Зняття з реєстрації трудових договорів між фізичними особами-підприємцями і найманими працівниками, зареєстрованими в СЗ до 01.01.2015 року.

11. Надання комплексу спеціальних послуг у розв'язанні проблеми роботи із трудовим колективом в ситуації запланованого вивільнення працівників.

12. Допомога у підготовці текстів оголошень про вільні робочі місця (вакансії) для їх розміщення у ЄІАС, засобах масової інформації і пошук кадрів.

13. Сприяння у проведенні роботодавцями співбесід із кандидатами на робочі місця та організація зустрічей з шукачами роботи, у тому числі у центрах зайнятості.

14. Проведення семінарів для роботодавців, у тому числі з питань працевлаштування інвалідів.

15. Надання консультацій щодо виконання певних норм законодавства про працю і зайнятість, державне соціальне страхування на випадок безробіття, у тому числі з питань вивільнення працівників, працевлаштування громадян, які не здатні конкурувати на ринку праці, з питань використання праці іноземців тощо.

16. Надання консультацій особам з питань організації та провадження підприємницької діяльності.

Підприємства мають можливість підготувати персонал з числа претендентів на вакансію з урахуванням вимог конкретного робочого місця: навчання відбувається за індивідуальними навчальними планами та програмами з урахуванням специфіки виробництва, в тому числі стажування; за рахунок зменшення обсягу теоретичного курсу скорочується загальний термін навчання; виробниче навчання і практика організуються відповідно до особливостей виробництва; ефективності навчання сприяє залучення наставників, досвідчених висококваліфікованих працівників, представників трудових династій; стажування надає можливість претендентам на вакансію набути й удосконалити знання, практичні уміння та навички у межах наявної професійної освіти безпосередньо на конкретному робочому місці або посаді або спорідненого підприємства або набути додаткової компетенції тощо.

Роботодавці беруть участь в розробці робочих навчальних планів і програм, які відображатимуть сучасні технології та особливості виробництва. За період професійного навчання на підприємстві особи зможуть адаптуватися до трудового колективу і швидше закріпитися на новій роботі після його закінчення. Професійне навчання організовується за рахунок коштів Фонду загальнообов`язкового державного соціального страхування України на випадок безробіття.

Центри зайнятості організовують підвищення кваліфікації шляхом стажування на виробництві. Стажування – це різновид підвищення кваліфікації

робітників і фахівців з вищою освітою з метою засвоєння особою кращого вітчизняного чи зарубіжного досвіду, набуття практичних умінь і навичок й додаткової компетенції щодо виконання обов'язків на займаній посаді або на посаді, на яку претендує безробітний. Стажування здійснюється на договірній основі терміном до трьох місяців в залежності від складності професії за індивідуальними планами, з урахуванням специфіки виробництва, використанням сучасних технологій.

Складовими стажування є:

- вивчення і засвоєння безробітними громадянами кращого вітчизняного й закордонного досвіду, пов`язаного з впровадженням нових технологій до виробництва, нової техніки, прогресивних форм організації праці;
- набуття та удосконалення знань, практичних умінь і навичок, у межах наявної професійної освіти, безпосередньо на конкретному робочому місці або посаді підприємства;
- удосконалення професійного рівня і ділових якостей щодо самостійного прийняття рішень з управлінських й виробничо-технічних проблем;
- набуття додаткової компетенції (оволодіння навичками користування сучасними засобами оргтехніки, зв`язку) тощо.

До проведення стажування залучаються наставники, досвідчені висококваліфіковані працівники. Така форма професійного навчання допоможе особі краще адаптуватись до трудового колективу, ознайомитися з особливостями виробництва, а набуті знання і вміння дозволять закріпитися на робочому місці, нададуть можливість кар'єрного зростання.

Під час навчання Полтавський обласний центр зайнятості надає: матеріальну допомогу у період професійного навчання відповідно до законодавства України; компенсує фактичні витрати на проїзд до місця навчання і назад; забезпечить безоплатне проживання у гуртожитку, у разі, коли професійне навчання організоване не за місцем постійного проживання особи.

Скориставшись цією соціальною послугою, роботодавці матимуть змогу: забезпечити підприємство, установу чи фірму висококваліфікованими

фахівцями; покращити якість продукції або послуг; зберегти конкурентоспроможність підприємства.

Також роботодавці мають можливість обрати потрібну форму професійного навчання осіб з числа претендентів на вакансію з урахуванням вимог певного робочого місця і перспектив розвитку підприємства, а саме: професійну підготовку або перепідготовку за робочими професіями як за груповою, так і за індивідуальною формою навчання, зокрема, безпосередньо на виробництві; підвищення кваліфікаційного рівня робітників (розряду, класу, категорії); підвищення кваліфікації спеціалістів; стажування робітників і спеціалістів, за потреби – безпосередньо на виробництві.

Роботодавці можуть брати безпосередню участь в організації професійного навчання: у складанні і погодженні робочих навчальних планів і програм; у роботі державної кваліфікаційної комісії; в організації виробничого навчання і практики осіб на певному робочому місці.

Науковцями, які досліджували питання ефективності політики зайнятості та її особливості в умовах ринкової економіки є: В. Г. Федоренко, О. В. Бражко, В. І. Герасимчук та інші [26, 33, 68, 69].

Із розвитком інформаційних технологій діяльність державної служби зайнятості спрямована, в основному, на адаптацію традиційних методів і технологій обслуговування суб’єктів-учасників ринку праці до умов нового часу.

Полтавський обласний центр зайнятості має здійснювати такі основні заходи:

1) ефективно і своєчасно реагувати на зміни зовнішніх умов, намагаючись зберегти стабільність на ринку праці за рахунок, або ліквідації впливу цих факторів, або пристосовуючись до них;

2) виконувати функції суб’єкта та інструмента державного регулювання, узгодження своєї політики з Урядом, отримуючи на це відповідні ресурси;

3) виконання лідерських функцій посередника у відносинах між роботодавцями, працівниками, органами місцевого самоврядування з питань регулювання ринку праці та сприяння працевлаштуванню населення.

Для реалізації вищезазначених заходів діяльність Полтавського обласного центру зайнятості на сьогодні спрямована на: впровадження єдиної технології надання соціальних послуг населенню; впровадження єдиної інформаційно-аналітичної системи; створення умов і системи підвищення кваліфікації кадрів на базі інституту підвищення кваліфікації.

Отже, Полтавський обласний центр зайнятості реалізує державну політику зайнятості, працюючи з громадянами та роботодавцями. Для успішної роботи місцевих центрів застосовується Єдина технологія обслуговування незайнятого населення, детальний опис якої подано далі.

2.2 Єдина технологія обслуговування незайнятого населення як основа роботи Полтавського обласного центру зайнятості

Наприкінці 2002 року Полтавський обласний центр зайнятості, як і всі центри зайнятості України, перейшов на роботу за новою технологією – Єдиною технологією обслуговування незайнятого населення (ЄТОНН), яка є передовим, єдиним такого масштабу напрацюванням у соціальній сфері. Робота за ЄТОНН передбачає уніфікацію всіх процесів діяльності служби зайнятості та спрямованість на ефективне обслуговування населення і роботодавців, дає змогу збільшити кількість відвідувачів, позбавитись черг, покращити умови надання послуг клієнтам [51].

Основна мета Єдиної технології обслуговування незайнятого населення – створення важливого елементу нової адаптованої до умов ринку системи соціального захисту і самозахисту населення; підвищення ефективності роботи державної служби зайнятості щодо надання соціальних послуг безробітним громадянам і роботодавцям [51].

Підґрунтям технології є дотримання таких принципів організації роботи персоналу як спеціалізація і кооперування праці, пропорційність і синхронність і безперервність. Слід підкреслити, що її основу складає набір стандартних

матеріальних умов праці і типізованих трудових процесів та організації праці співробітників центрів зайнятості стандартизація і уніфікація форм документації, типізація.

Значному підвищенню продуктивності праці спеціалістів, забезпеченню покращення якості послуг клієнтам, збільшенню пропускної можливості служби зайнятості в цілому сприятимуть рекомендації щодо організації праці та відпочинку співробітників центрів зайнятості та заходів профілактики втоми і професійних захворювань, які базуються на рекомендаціях з фізіології і гігієни праці.

Технологія дозволяє забезпечити високу працездатність і продуктивність діяльності персоналу без його перевтоми і розвитку професійних захворювань.

Всі функції спрямовані на оперативне і якісне надання послуг клієнтам служби зайнятості і мають виконуватись незалежно від категорії центру, чисельності спеціалістів і матеріально-технічного оснащення. Засоби їх виконання залежать від наявних умов і вирішуються безпосередньо директором центру зайнятості базового рівня. Зміни і доповнення до технології вносяться на підставі наказу державного центру зайнятості.

При розробленні цієї технології був застосований досвід кращих вітчизняних ЦЗ, досвід зарубіжних країн – Великобританії, Німеччини, Данії, Польщі, Росії. Найбільш ефективні методи обслуговування незайнятого населення, інноваційні елементи технології були максимально адаптовані до вітчизняних умов, стандартизовані та уніфіковані.

Єдину технологію обслуговування незайнятого населення в центрах зайнятості України розробила творча група Інституту підготовки кадрів державної служби зайнятості, в якій працювали фахівці інституту, спеціалісти Державного, обласних, міських та районних центрів зайнятості, деяких наукових установ і навчальних закладів

Розглянемо принципи і засади єдиної технології обслуговування незайнятого населення в центрах зайнятості України. Технологія обслуговування незайнятих громадян в центрах зайнятості – це спосіб діяльності спеціалістів

державної служби зайнятості щодо надання клієнтам передбачених законодавством соціальних послуг на основі раціонального розподілу дій на скоординовані процедури й операції, визначення оптимальних засобів і методів їх виконання.

Технологія базується на загальновизнаних принципах діяльності служб зайнятості європейських країн. Основними є такі принципи:

– пріоритетність інтересів і потреб клієнтів служби зайнятості, урахування мотивів людини як особистості, її обставин, нахилів і здібностей;

– співробітництво клієнта і служби зайнятості - найбільш ефективний і короткий шлях до працевлаштування;

– пріоритетність послуг центру зайнятості, пов'язаних з пошуком і підбором роботи перед іншими видами послуг.

Засадами Єдиної технології обслуговування незайнятого населення в центрах зайнятості України є [51]:

1. Активізація власних зусиль клієнтів щодо влаштування свого життя, підвищення відповідальності людини перед собою, своєю сім'єю та суспільством: навчання клієнтів методам і техніці самостійного пошуку роботи; розроблення більшістю клієнтів за допомогою спеціалістів ЦЗ планів самостійного пошуку роботи; розширення кола інформації про вакантні місця шляхом створення єдиної національної інформаційної комп'ютерної системи і забезпечення вільного доступу кожного відвідувача до інформації про вакансії; створення в ЦЗ функціонального сектору самостійного пошуку вакансій; сприяння безробітним в їхніх зусиллях щодо започаткування власної справи; залучення незайнятих громадян до участі в оплачуваних громадських роботах; створення в ЦЗ функціонального сектору профінформування населення; підвищення відповідальності клієнтів за власні дії щодо пошуку роботи (інформування спеціалістів ЦЗ про проведену роботу).

2. Підвищення відповідальності фахівців ЦЗ за ефективність заходів, що використовувались, кінцеві результати роботи з клієнтами: обговорення на засіданні спеціально призначеної комісії центру зайнятості ефективності

заходів щодо сприяння влаштуванню кожного клієнта, який довгий час (від трьох до шести місяців) перебував на обліку в ЦЗ; використання результатів роботи спеціалістів при проведенні атестації, конкурсів на заміщення вакантних посад, формуванні резерву на висування, моральному і матеріальному заохоченні.

3. Зміцнення взаємодії з роботодавцями – підвалини підвищення ефективності діяльності центрів зайнятості: інформування роботодавців у відповідності із профілем підприємств про професійно-кваліфікаційний склад осіб, які зареєстровані в ЦЗ; вивчення потреб роботодавців і надання допомоги щодо укомплектування підприємств персоналом і професійне навчання кадрів на їхнє замовлення з числа незайнятого населення; консультування з питань впровадження деяких норм законодавства про працю і зайнятість; здійснення на замовлення роботодавців підбору необхідних працівників з використанням психодіагностичних методик; інформування про стан, основні тенденції і процеси на локальному ринку праці; інформування про витрати ЦЗ коштів страхового фонду з розкриттям досягнутого ефекту по кожній статті бюджету.

4. Раціоналізація розподілу персоналу служби зайнятості і використання його робочого часу: розподіл персоналу з урахуванням його «навантаження», (кількості незайнятого населення, яка припадає на одного працівника ЦЗ); визначення норм часу на здійснення технологічних операцій і процедур, впровадження системи автоматизованого нарахування всіх видів допомоги; спеціалізація і взаємозамінність фахівців ЦЗ на основі розподілу здійснюваних операцій на прості і добре уявлені елементи; зосередження уваги фахівців, які безпосередньо працюють з клієнтами, виключно на виконанні своїх функціональних обов'язків завдяки автоматизації статистичного обліку та організації ефективної системи документообігу; розроблення для кожного спеціаліста детальної посадової інструкції.

5. Розподіл потоків клієнтів залежно від мети відвідування центру зайнятості: створення в ЦЗ диспетчерсько-консультаційного сектору, покладення на одного з фахівців диспетчерсько-консультаційних функцій; розміщення робочих

приміщень у ЦЗ відповідно до технології обслуговування конкретних категорій клієнтів; виділення в окреме технологічне поле роботи по виконанню замовлень на підготовку довідок клієнтам.

6. Розподіл приміщень ЦЗ на функціональні сектори, в яких, незалежно від площі приміщень, особливостей будинку ЦЗ, здійснюються визначені процедури і операції щодо обслуговування клієнтів: створення великих просторових зон, де клієнтам можуть надаватися декілька послуг, в першу чергу тих, які спрямовані на активізацію їх власних зусиль щодо влаштування свого життя; уніфіковане за змістом інформаційне наповнення приміщень ЦЗ, яке дозволяє клієнтам самостійно одержати максимум інформації, а також допомагає їм чітко уявити свої права та обов'язки.

Найважливішою засадою побудови ЄТОН є розподіл клієнтів центру зайнятості на певні категорії:

1. Працездатні громадяни працездатного віку, які не мають роботи і вперше звернулися до центру зайнятості або перебували на обліку і були зняті з обліку в зв'язку з працевлаштуванням та повторно звернулися до ЦЗ.

2. Громадяни, які зареєстровані як такі, що шукають роботу і звернулись до центру зайнятості в призначений день.

3. Громадяни, які раніше перебували на обліку в центрі зайнятості як безробітні (крім зареєстрованих на підставі п.1 ст.26), були зняті з обліку за власною заявою або в зв'язку з невідвідуванням центру зайнятості більше одного місяця, не працевлаштувалися і повторно звернулись до центру зайнятості протягом двох років з моменту першої реєстрації.

4. Громадяни, які зареєстровані як безробітні і звернулись до центру зайнятості в призначений час.

5. Громадяни, які працюють і бажають змінити місце роботи або шукають додаткову зайнятість (додатковий заробіток).

6. Інваліди, які бажають працевлаштуватися.

7. Громадяни, які звернулися до центру зайнятості за довідками.

8. Керівники, які звернулись до центру зайнятості з метою реєстрації підприємств як платників внесків до Фонду загальнообов'язкового державного соціального страхування України на випадок безробіття (ФЗДССУВБ).

9. Керівники і працівники кадрових служб підприємств, що звернулись до центру зайнятості за допомогою в підборі персоналу.

10. Роботодавці, які не мають прав юридичної особи і звернулися до ЦЗ щодо реєстрації трудових договорів між працівником і фізичною особою.

Такий підхід обумовлений різницею у змісті технологічних процедур і операцій, що виконують певні фахівці центрів зайнятості при наданні тієї чи іншої послуги.

При визначенні процедур щодо обслуговування тієї чи іншої категорії громадян, послідовності операцій враховувались різні обставини, що можуть виникати у клієнтів, обумовлювати багатоваріантність можливого розвитку подій та впливати на зміст дій спеціалістів ЦЗ. Відповідно до цих обставин пропонуються варіанти дій фахівців.

Отже, запропоновано поділ клієнтів, який дозволяє запроваджувати цілеспрямовані дії спеціалістів центру зайнятості, перш за все, залежно від потреб клієнтів і ознак ситуації. Це допомагає також чітко визначити зміст операцій, їх послідовність, розподілити функції і обов'язки між співробітниками центру зайнятості, здійснити нормування часу на операції і процедури, регламентує зміст їх дій, що допомагатиме фахівцям надавати більш якісні послуги клієнтам.

У 1998 році відповідно до «Національної програми інформатизації» 1998 року Полтавський обласний центр зайнятості розпочав упровадження Єдиної інформаційно-аналітичної системи служби зайнятості України (ЄІАС), що базується на сучасних Інтернет-Intranet технологіях [42]. Це дало змогу підняти рівень соціального захисту населення від безробіття на якісно новий щабель.

ЄІАС – це глобальна інформаційна система, яка об'єднає всі центри зайнятості, розподіливши функції між ними за ієрархією. Частина функцій з

місцевого рівня перейде на обласний і ще вище – на державний, що дозволить вивільнити працівників базових центрів для безпосередньої роботи з населенням. З 1 липня 2003 року розпочато серійне впровадження ЄІАС у центрах зайнятості України.

Спосіб доведення інформації до суб'єктів служби зайнятості і працевлаштування клієнтів служби зайнятості (Єдина інформаційно-аналітична система) визнаний департаментом інтелектуальної власності як винахід з надання державних соціальних послуг.

У серпні 2003 року Державна служба зайнятості України стала 92-м членом Світової Асоціації громадських служб зайнятості. Вступ в Асоціацію сприятиме руху України на шляху подальшої інтеграції до Європейського Союзу, підвищенню громадського іміджу служби зайнятості України. Членство в цій міжнародній організації дозволило Україні вивчати і використовувати досвід тих країн, служби зайнятості яких створені та функціонують вже тривалий час. Практичне застосування методів і програм, розроблених членами Асоціації, дало змогу Державній службі зайнятості України досягти нових успіхів у боротьбі з безробіттям і підвищенні рівня соціального захисту населення.

Основною метою створення Єдиної інформаційно-аналітичної системи «Служба зайнятості України» є забезпечення:

- реалізації державної політики зайнятості населення, професійної орієнтації, підготовки і перепідготовки, працевлаштування і соціальної підтримки громадян, тимчасово незайнятих трудовою діяльністю;

- аналізу і прогнозу попиту і пропозиції на робочу силу, інформування населення і державних органів врядування про стан ринку праці;

- ефективної участі у підготовці державних і територіальних Програм зайнятості населення.

ЄІАС СЗУ призначена для інформаційної підтримки і автоматизації ділових процесів: надання соціальних послуг шукачам роботи і роботодавцям за єдиною технологією обслуговування клієнтів державної служби зайнятості

України; ведення статистичних спостережень, аналітичних досліджень і прогнозування стану ринку праці України; розробки і контролю виконання Програми зайнятості населення; роботи з платниками до Фонду загальнообов'язкового державного соціального страхування України на випадок безробіття і контролю грошових надходжень до цього фонду; фінансового планування та аналізу стану матеріально-технічної бази Служби зайнятості України.

ЄІАС СЗУ функціонує більш ніж у 650 центрах зайнятості районного, регіонального і державного рівнів. Користувачами ЄІАС СЗУ є близько 13 000 співробітників ДСЗУ, а також велика кількість Інтернет-користувачів. Основною метою створення ЄІАС СЗУ був перехід від системи фіксації подій до системи підтримки ділових процедур, що виконуються у центрах зайнятості Державної служби зайнятості України.

Критерії побудови ЄІАС СЗУ подані на рисунку 2.3.

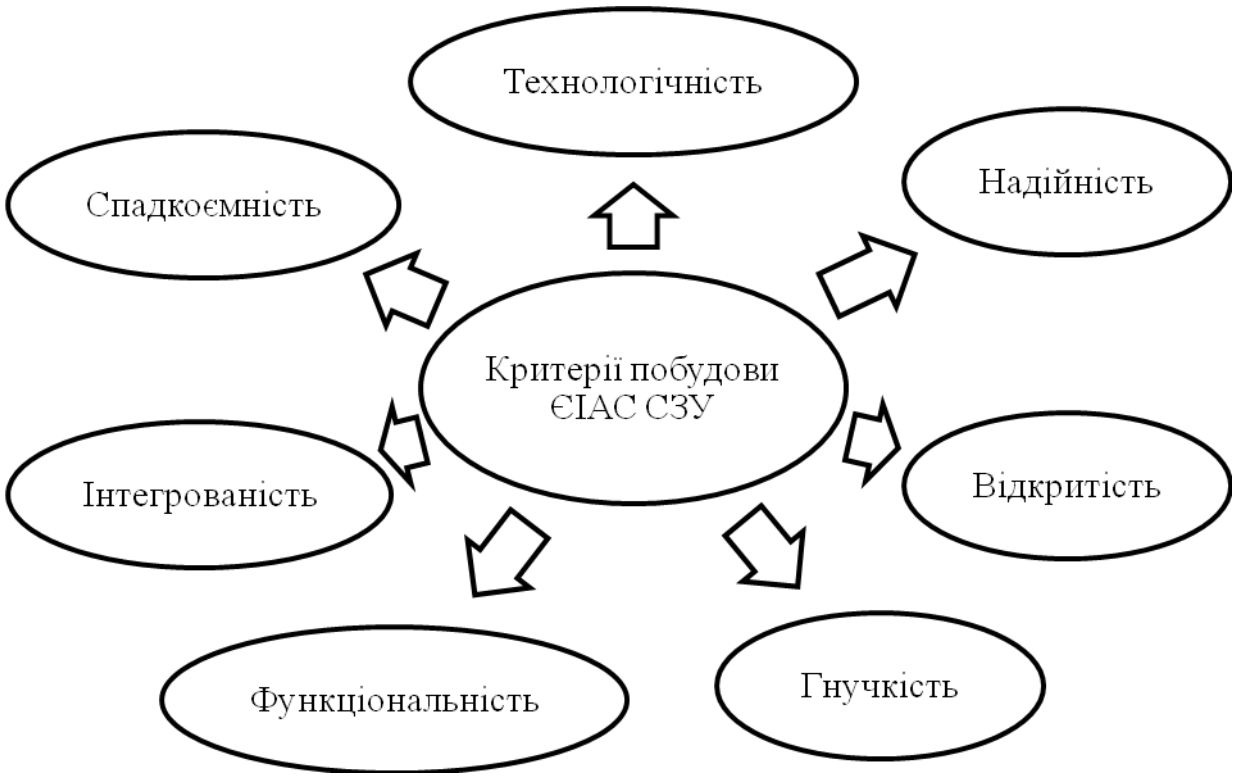

Рисунок 2.3 – Критерії побудови Єдиної інформаційно-аналітичної системи «Служба зайнятості України», складено автором за [42]

ЄІАС СЗУ складається з таких компонентів:

– група підсистем «Соціальні послуги та Фонд», засобами якої реалізовані механізми підбору роботи для шукаючих роботу, створені єдині для всієї України довідники населених пунктів, підприємств, платників до фонду, навчальних закладів тощо, створена та підтримується в актуальному стані (за допомогою механізмів поштової реплікації даних) всеукраїнська база вакансій і громадян, що звернулися до СЗУ.

– група підсистем «Інформування» (рис. 2.4), засобами якої реалізована можливість надання додаткових послуг особам, що шукають роботу та роботодавцям через Інтернет.

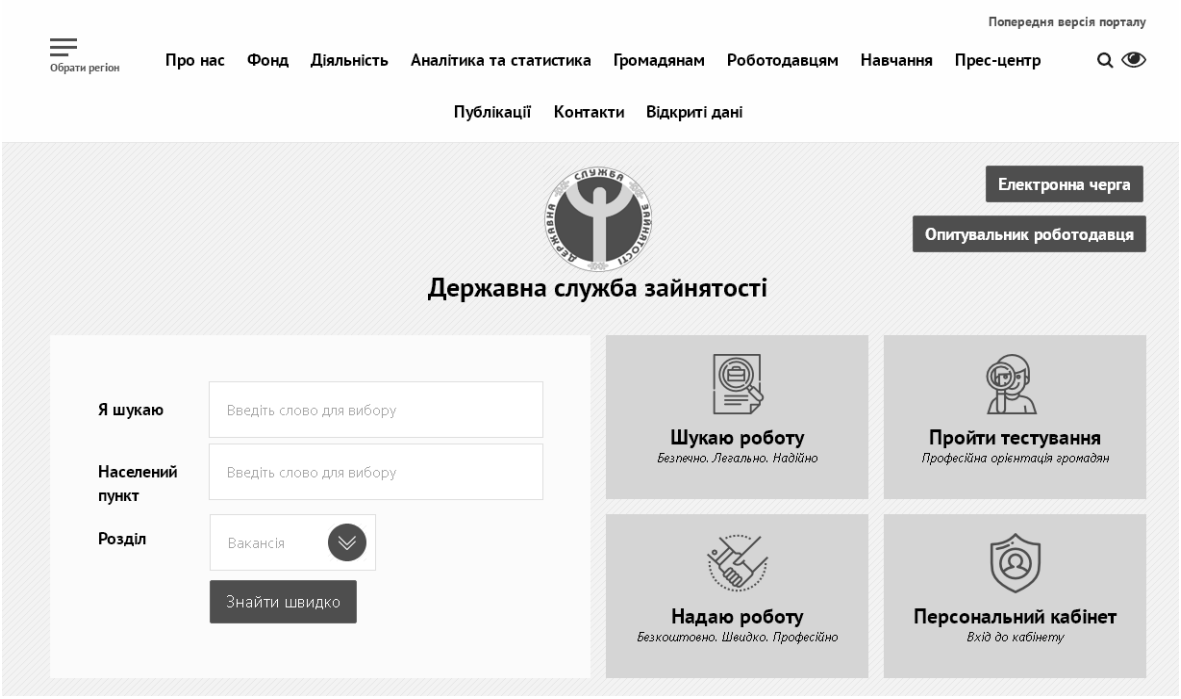

Рисунок 2.4 – Початкова веб-сторінка Інтернет-порталу Державної служби зайнятості України [39]

– група підсистем «Бюджетування», засобами якої спрощені процеси формування бюджетних планів щодо надходжень та витрат з ФЗДССУВБ, реалізовані механізми введення даних розподілу та контролю за використанням коштів ФЗДССУВБ по статтям кошторису на рівнях Державний центр зайнятості, Регіональний центр зайнятості та Базовий центр зайнятості.

– група підсистем «Бухгалтерський облік та аналітика фінансової діяльності», засобами якої автоматизовані процеси бухгалтерського обліку, що полегшує та прискорює підготовку первинних бухгалтерських документів та реєстрацію господарських операцій, зберігання та обробку цієї інформації.

– група підсистем «Облік робочого часу та заробітна платня», засобами якої реалізовані механізми планування та обліку робочого часу працівників Державної служби зайнятості України, розрахунку та обліку виплати заробітної плати.

– група підсистем «Діловодство», засобами якої автоматизовані процеси документообігу, що сприяє ефективному вирішенню задач у розрізі контролю і виконання завдань.

Принципи побудови ЄІАС подані на рисунку 2.5.

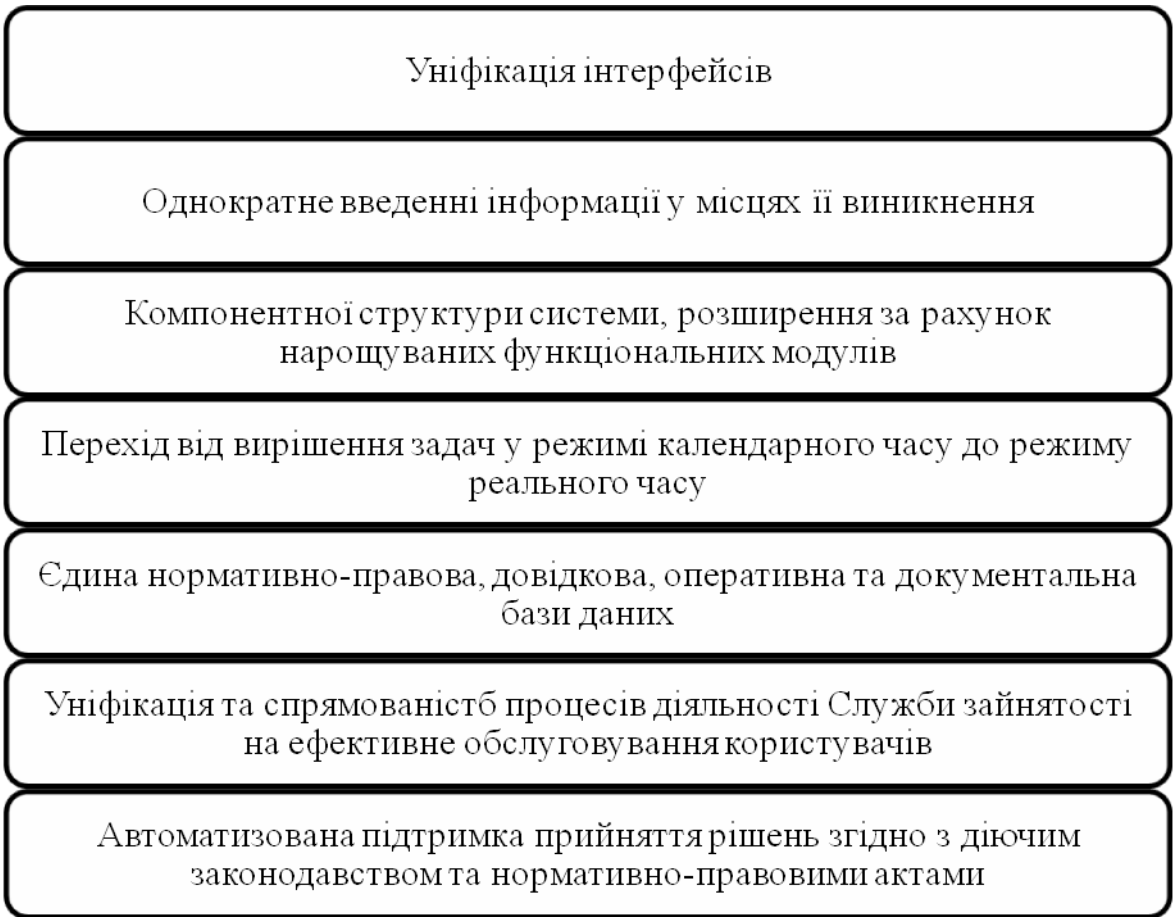

Рисунок 2.5 – Принципи побудови ЄІАС «Служба зайнятості України», складено автором за [42]

Принципи побудови ЄІАС полягають в: уніфікації інтерфейсів користувача; однократному введенні інформації у місцях її виникнення; забезпеченні компонентної структури системи, що передбачає можливість розширення за рахунок нарощуваних функціональних модулів; переході від вирішення задач у режимі календарного часу до режиму реального часу; використанні єдиної нормативно-правової, довідкової, оперативної і документальної бази даних; уніфікації і спрямованості всіх процесів діяльності Служби зайнятості на ефективне обслуговування користувачів; автоматизованій підтримці прийняття рішень згідно з діючим законодавством і нормативно-правовими актами.

До функціонального складу ЄІАС СЗУ входять технологія діяльності служби зайнятості, координація і нормативи, життєдіяльність служби та інтегрована база даних (рисунок 2.6).

Рисунок 2.6 – Функціональний склад ЄІАС «Служба зайнятості України», скриншот [42]

Технологія діяльності служби містить модулі, що відповідають основним завданням служби зайнятості, серед яких організація прийому та обслуговування громадян, робота з роботодавцями та навчальними закладами.

Інформаційна підтримка функцій ЄІАС складається з трьох рівнів: державного, регіонального та базового, між якими відбувається обмін даними (рисунок 2.7).

Рисунок 2.7 – Інформаційна підтримка функцій ЄІАС СЗУ, скриншот [42]

Базовий рівень підтримки забезпечується роботою з оперативною базою безробітних у визначеному районі, вакансій, роботодавців та платників Фонду. Інформація з районних баз збирається та обробляється на наступному рівні – регіональному, де робиться регіональний зріз за визначеними показниками. У свою чергу інформація передається до баз державного рівня, де формуються єдині всеукраїнські бази безробітних, вакансій, навчальних закладів, професій, роботодавців та інші. Таким шляхом інформація акумулюється від базового до державного рівня, що дає можливість оцінити реальний стан та скоординувати державну політику зайнятості з урахуванням сучасних тенденцій.

Для керівників центрів зайнятості надається інформаційна підтримка прийняття рішень на різних рівнях та з різних питань. Ця особливість ЄІАС СЗУ дає можливість дотримання єдиної політики в усіх регіонах України. Модулі прийняття рішень розподілені відповідно до рівнів (рисунок 2.8).

Рисунок 2.8 – Інформаційна підтримка керівника Служби зайнятості України, скриншот [42]

Впровадження цієї технології дало змогу скоротити час службовців Полтавського обласного центру зайнятості, що витрачався на узгодження потреб роботодавців стосовно вимог до працівників і характеристик (кількісних і якісних) трудових ресурсів, що пропонуються на ринку праці. Автоматизація спростила б функції Полтавського обласного центру зайнятості, концентруючи її увагу на поповнення інформаційної бази даних стосовно попиту і пропозицій на працю та на контроль за функціонуванням цієї системи. Утворення такої системи мереж по всій країні дозволить не лише зробити ринок праці цілісним, забезпечуючи просте працевлаштування на всій території, але і надасть можливість оцінки стану ринку праці на загальнодержавному рівні, зводячи показники місцевих центрів зайнятості.

Слід зазначити, що серед безробітних кожен другий займав місце робітника, кожний третій – посаду службовця, а кожний шостий безробітний взагалі не має професійної підготовки.

Функцію інтелектуалізації кадрового потенціалу державної служби зайнятості виконує Інститут підготовки кадрів державної служби зайнятості України (далі Інститут). Діяльність останнього стосовно розробки програм підготовки кадрів СЗ має здійснюватися на основі оцінки потреби ринку праці у таких кадрах відповідної спеціальності, кваліфікації. Також злагоджена робота Інституту та ЄІАС може забезпечити навчання в режимі «on-line». Щоправда таке «перепрофілювання» кадрів потребує глибоких досліджень, реформувань. Доступ трудових ресурсів СЗ, що навчаються, до електронних джерел інформації має риси самоосвіти, наявність заходів контролю рівня знань (тестувань, практичних занять тощо) частково зменшить потребу у навчальному персоналі Інституту, але з іншого боку спрямує його роботу в ефективніше русло – на практичну діяльність в плані навчання. Проте, спочатку, варто лише частково запровадити «пробний варіант» цієї системи та через деякий час оцінити її ефективність. У разі позитивних результатів процедуру можна запроваджувати повністю.

Ще однією перевагою такої системи підготовки кадрів СЗ є доступ до джерел навчального матеріалу не в самому Інституті, а і поза ним (так зване Інтернет-навчання). Невід'ємною складовою навчання має стати практика. Оцінка результатів навчання складається з двох частин:

І – перевірка знаньв режимі «on-line», але не в мережі Інтернет, а в межах ЄІАС в структурних підрозділах Інституту;

ІІ – оцінка практичних навичок трудових ресурсів СЗ навчальним персоналом Інституту.

Вже на основі попередніх етапів оцінок здійснюється загальна оцінка результатів навчання.

Таким чином, запровадження ЄІАС – стало лише першим кроком на шляху удосконалення і модернізації роботи Полтавського обласного центру зайнятості для забезпечення ефективнішого функціонування ринку праці в Україні. З одного боку, така диверсифікована інформаційна система потребувала значних витрат на своє обслуговування, але лише на початковому етапі. Через деякий

час після налагодження її роботи отримується позитивний результат і скорочення витрат на оплату робочого часу працівників Полтавського обласного центру зайнятості, оскільки автоматизація зменшить потребу в них.

Особливістю запровадження такої технології обслуговування учасників ринку праці є активізація ініціативи власної зайнятості в бажаному варіанті самих клієнтів та оцінка власних можливостей. Реформування системи підготовки кадрів поряд із удосконаленням ЄІАС створить передумови для розвитку інтелектуалізованого, освіченого суспільства, ефективної та швидкої зайнятості, доведення рівня безробіття до мінімального значення.

2.3 Документно-інформаційна система «Соціальні послуги та Фонд» Єдиної інформаційно-аналітичної системи державної служби зайнятості

Усі фахівці ДСЗ працюють з групою підсистем «Соціальні послуги та Фонд» Єдиної інформаційно-аналітичної системи державної служби зайнятості. Щороку у зв’язку зі змінами чинного законодавства і реформуванням системи соціальних послуг здійснюється модифікація існуючих алгоритмів і функцій ЄІАС ДСЗ, для забезпечення безперебійної роботи постійно триває її технічне супроводження і підтримка роботи користувачів.

ЄІАС ДСЗ – веб-орієнтована система, яка побудована з використанням передових технологій у сфері інформаційних систем. ЄІАС ДСЗ розроблена з урахуванням складної трьохрівневої організаційної структури і територіального розташування великої кількості установ різного рівня підпорядкування. Користувачами системи є близько 12 000 співробітників Державної служби зайнятості. Інформація з ЄІАС ДСЗ надається та використовується відповідно до законів України «Про інформацію» та «Про захист персональних даних».

В ЄІАС ДСЗ автоматизовано понад 2500 функцій, що згруповані у такі підсистеми:

1. Організація прийому громадян, які звернулися до центру зайнятості. Засобами підсистеми підтримуються процеси обліку прийомів громадян, які звернулися до центру зайнятості, ведення прийомів, ведення реєстру завдань для діловодів щодо перенесення персональних справ громадян до робочих місць спеціалістів тощо (рисунок 2.9).

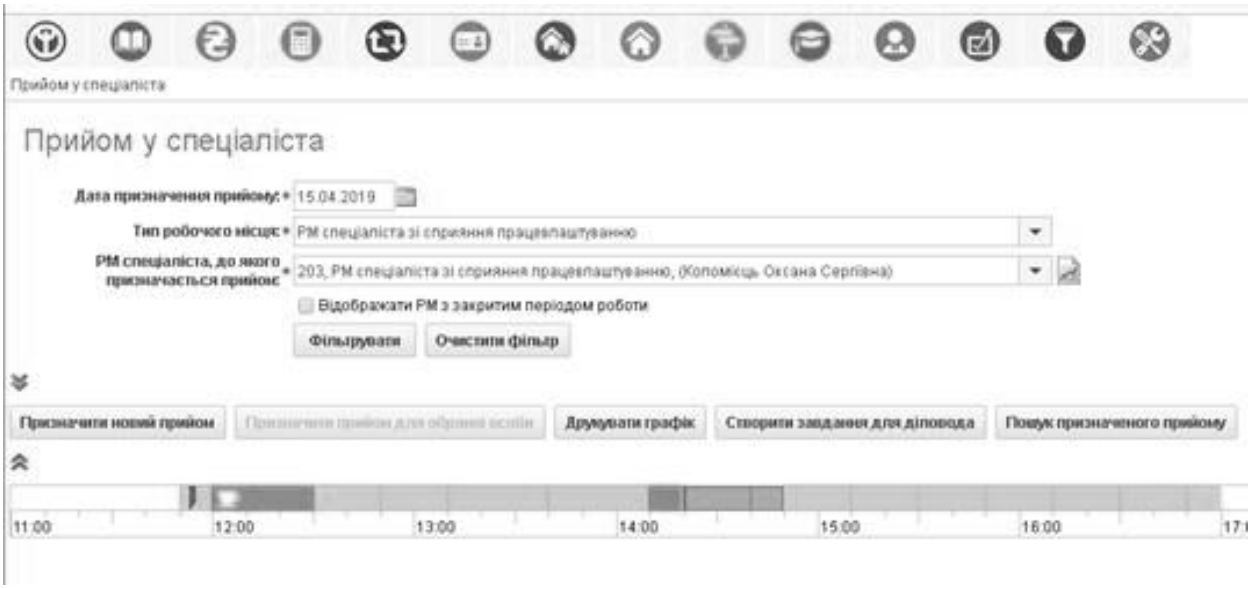

Рисунок 2.9 – Вікно програми ЄІАС СЗУ «Прийом у спеціаліста», скриншот [42]

2. Підтримка організації прийому громадян у базових центрах зайнятості засобами електронного табло. Засобами підсистеми підтримується процес інформування громадянина щодо початку прийому у спеціаліста центру зайнятості.

3. Реєстрація та надання послуг особам, які звернулися до центру зайнятості. Засобами підсистеми підтримуються процеси ведення персональної справи та картки громадянина, ведення послуг, наданих громадянину у службі зайнятості. Зокрема, підтримується процес організації та надання послуг особам в незалежності від зареєстрованого місця проживання та перебування.

4. Взаємодія з роботодавцями. Засобами підсистеми підтримуються процеси надання послуг роботодавцям та реєстрація цих послуг: укомплектування вакансій, контроль за працевлаштуванням громадян на підприємствах,

компенсація ЄВ, компенсація на оплату праці внутрішньо переміщеним особам, облік пропозицій за цивільно-правовим договором тощо.

5. Організація громадських та інших тимчасових робіт. Засобами підсистеми підтримуються процеси укладання договорів між центром зайнятості та підприємством на організацію громадських робіт, направлення громадян на громадські роботи, контроль за виконанням громадських робіт, ведення пропозицій тимчасових робіт тощо.

6. Організація працевлаштування на постійне місце роботи. Засобами підсистеми підтримуються процеси підбору підходящої роботи громадянам, видачі направлення на роботу, реєстрація результату працевлаштування, процеси підбору та працевлаштування осіб за цивільно-правовим договором, укладеним за сприяння служби зайнятості тощо.

7. Ведення добового наказу та прийняття рішень по безробітним. Засобами підсистеми підтримуються процеси прийняття рішень по безробітним громадянам та їх затвердження у добовому наказі.

8. Нарахування, утримання та виплати безробітним. Засобами підсистеми підтримуються процеси нарахування матеріальної допомоги безробітним, здійснення утримань, формування відомостей до сплати нарахованих коштів, формування реєстрів для здійснення верифікації та моніторингу достовірності інформації, поданої фізичними особами для нарахування та отримання соціальних виплат, пільг, субсидій, пенсій, заробітної плати, інших виплат, що здійснюються за рахунок коштів державного та місцевих бюджетів, коштів Пенсійного фонду України, фондів загальнообов’язкового державного соціального страхування, ведення заявок на фінансування нарахованої допомоги.

9. Організація професійного навчання. Засобами підсистеми підтримуються процеси укладання договорів між центром зайнятості та навчальним закладом про професійне навчання безробітних у навчальному закладі, укладання договорів між центром зайнятості та особами на професійне навчання, укладання договорів між центром зайнятості та роботодавцем про організацію

професійного навчання безробітних на замовлення роботодавця, прийому заявок від зареєстрованих безробітних громадян на професійну підготовку, перепідготовку, підвищення кваліфікації, направлення на професійне навчання, контроль за проходженням громадян професійного навчання, укладання трьохсторонніх договорів між центром зайнятості, особою та роботодавцем про професійне навчання безробітного у роботодавця, підтвердження неформального навчання, видачі ваучерів на перепідготовку, спеціалізацію підвищення кваліфікації, підготовку на наступному освітньо-кваліфікаційному рівні.

10. Обмін даними з державними установами. Засобами підсистеми підтримуються процеси обміну даними з: Пенсійним фондом України, Міністерством соціальної політики України, Державною фіскальною службою, Державною казначейською службою України, Міністерством фінансів України.

11. Статистика та аналітика. Засобами підсистеми підтримується процеси формування статистичної та аналітичної звітності щодо стану ринку праці та надання послуг населенню та роботодавцям.

12. Організація роботи центру зайнятості. Засобами підсистеми підтримуються процеси обліку працівників центру зайнятості, обліку робочих місць центру зайнятості, формування звіту про навантаження спеціалістів центру зайнятості, автоматичне формування пам’яток для спеціалістів тощо (рисунок 2.10).

13. Ведення нормативно-довідкової інформації. Засобами підсистеми підтримується процес ведення довідників та класифікаторів, необхідних для забезпечення виконання функцій служби зайнятості України у центрах зайнятості.

14. Адміністрування. Засобами підсистеми підтримуються процеси обліку користувачів, керування правами доступу користувачів до функцій системи у відповідності до ролей користувача, ведення журналів з інформацією про зміни, внесені користувачами до БД групи підсистем «Соціальні послуги та Фонд» ЄІАС ДСЗ.

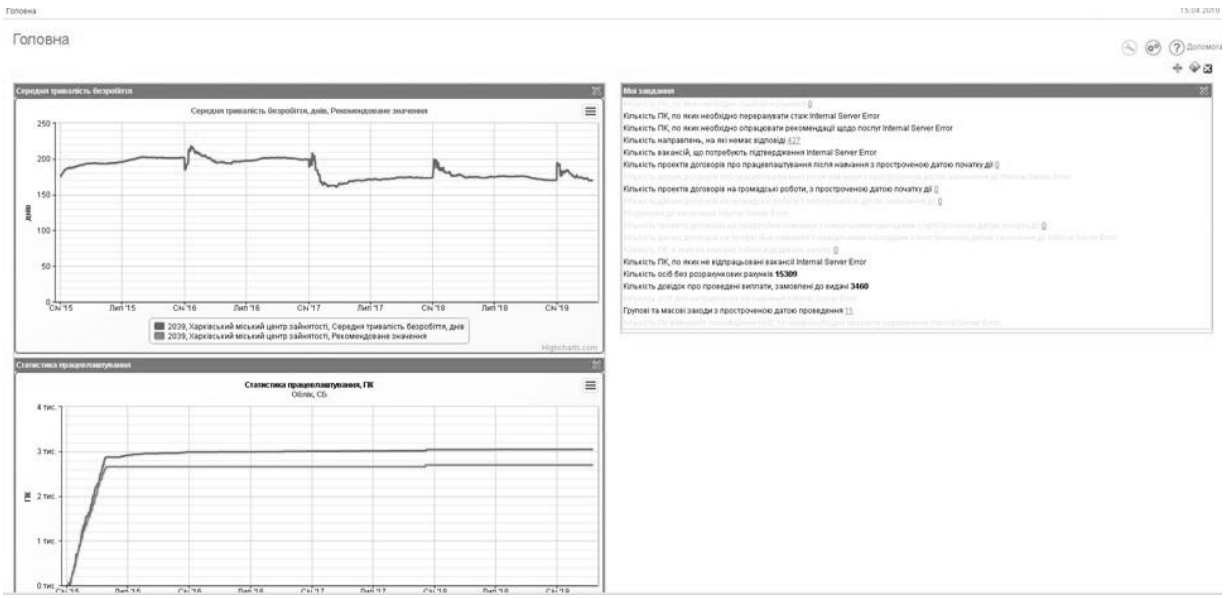

Рисунок 2.10 – Вікно програми ЄІАС СЗУ «Організація роботи центру зайнятості», скриншот [42]

15. Організація надання послуг населенню і роботодавцям засобами Touch Screen. Засобами підсистеми підтримується процес самостійного отримання консультаційних послуг та послуг з пошуку роботи громадянами і самостійного отримання консультаційних послуг і послуг з укомплектування вакансій роботодавцями.

16. Інтеграція з Електронною чергою, веб-сайтом державної служби зайнятості «Єдине соціальне середовище зайнятості», електронним кабінетом пошукача роботи й електронним кабінетом роботодавця веб-сайту державної служби зайнятості «Єдине соціальне середовище зайнятості».

17. Універсальні фільтри забезпечують можливість миттєвого вибору з бази даних будь-якої інформації для проведення оперативного аналізу та прийняття управлінських рішень (рисунок 2.11).

Використання ЄІАС СЗУ забезпечує підтримку на трьох рівнях (центр, область, район) усіх технологічних процесів державної служби зайнятості (організація прийому і надання послуг громадянам, які шукають роботу, безробітним, взаємодія з роботодавцями, працевлаштування, профорієнтація, організація професійного навчання і громадських робіт, нарахування допомоги

по безробіттю, взаємодія з державними органами, формування статистичної звітності тощо).

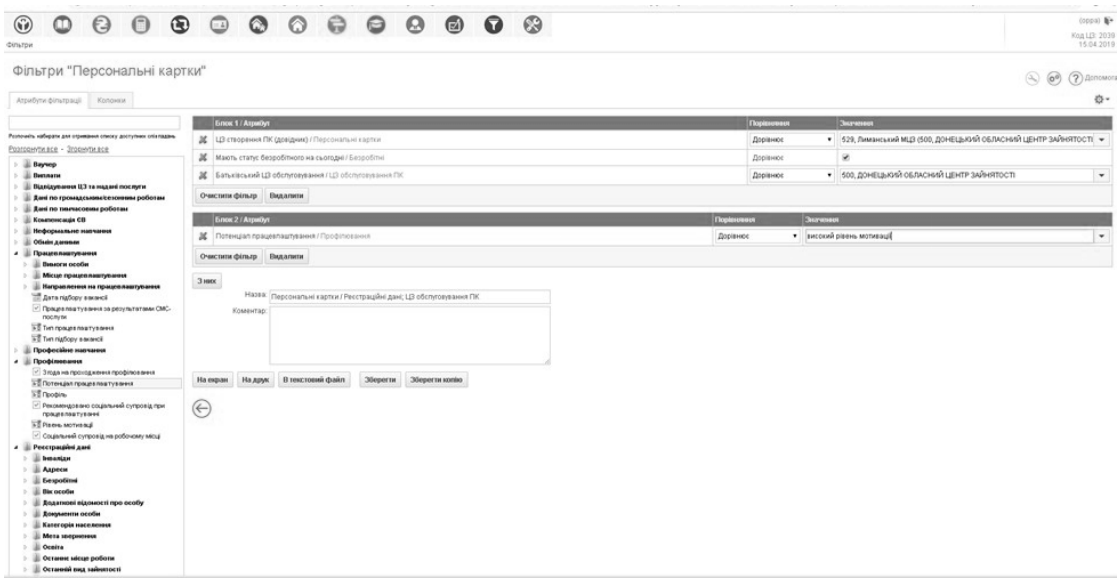

Рисунок 2.11 – Вікно програми ЄІАС СЗУ фільтри «Персональні картки», скриншот [42]

Усі перелічені вище підсистеми подані на рисунку 2.12.

Рисунок 2.12 – Підсистеми ЄІАС СЗУ, складено автором за [42]

ЄІАС СЗУ надає ефективні інструменти контролю за організацією та інформаційною підтримкою управлінських рішень щодо надання послуг безробітним, обліку персоналу і документообігу служби зайнятості; оперативно адаптується до нових законодавчих змін; забезпечує електронний міжвідомчий взаємообмін даними з Пенсійним Фондом України, Державною фіскальною службою України, Міністерством соціальної політики України, Міністерством фінансів України, що дозволяє уникнути розбіжностей даних при призначенні матеріального забезпечення, скоротити термін обробки масивів документів, зменшити обсяги обігу паперових документів.

Щороку в базі даних ЄІАС СЗУ обліковується більше 1 млн. вакансій та біля 1 млн. безробітних. Щоденно в системі приймається понад 15 000 рішень щодо осіб, виконується понад 50 000 розрахунків виплат та утримань безробітним, понад 25 000 розрахунків для компенсації ЄСВ роботодавцям. Щоденно здійснюється понад 12 000 онлайн запитів щодо осіб до ПФУ та щомісячно здійснюється обмін щодо працівників – понад 800 тис. записів. Щомісячно обробляється близько 30 тис. запитів для обміну з Мінсоцполітики [33].

Таким чином, було досягнуто основної мети створення Єдиної інформаційно-аналітичної системи державної служби зайнятості, а саме, забезпечення:

- інформаційної підтримки реалізації державної політики у сфері зайнятості населення;
- створення цілісної системи інформаційної взаємодії державних органів влади, що здійснюють заходи щодо сприяння зайнятості населення;
- проведення моніторингу ринку праці, аналізу попиту та пропонування робочої сили;
- розвиток активних програм сприяння зайнятості населення;
- управління внутрішніми процесами ДСЗ [33].

Отже, робота центрів зайнятості України здійснюється з використанням інформаційної системи ЄІАС СЗУ, що об’єднує усі локальні центри в єдину державну мережу. Документно-інформаційна система установи сконцентрована у зазначеній вище інформаційній системі, тому питання її захисту є

надзвичайно актуальним. Далі у роботі розглянемо шляхи вдосконалення системи захисту центру зайнятості.

РОЗДІЛ 3 ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ДОКУМЕНТНО-ІНФОРМАЦІЙНОЇ СИСТЕМИ ПОЛТАВСЬКОГО ОБЛАСНОГО ЦЕНТРУ ЗАЙНЯТОСТІ

3.1 Порядок створення комплексної системи захисту документно-інформаційних ресурсів

Відповідальність за захист документно-інформаційної системи служби зайнятості згідно організаційної структури установи несе відділ інформаційних систем ЦЗ. У Полтавському обласному центрі зайнятості начальником відділу є Жуковський Сергій Володимирович.

Основними завданнями відділу інформаційних систем Полтавського обласного центру зайнятості зайнятості є (рисунок 3.1):

- технічне забезпечення функціонування міського центру зайнятості шляхом технічної підтримки апаратних засобів та впровадження нових програмних пакетів;
- надання консультативної допомоги спеціалістам міського центру зайнятості;
- виконання робіт з визначення вимог щодо захисту інформації в Єдиній інформаційно-аналітичній системі, а також з експлуатації, обслуговування, підтримки працездатності комплексної системи захисту інформації (СЗІ);
- контролю за станом захищеності інформації в ЄІАС.

Правову основу для діяльності відділу інформаційних систем Полтавського обласного центру зайнятості щодо захисту інформації становлять Закон України «Про захист інформації в автоматизованих системах», Положення про технічний захист інформації в Україні, «Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах» [33].

.

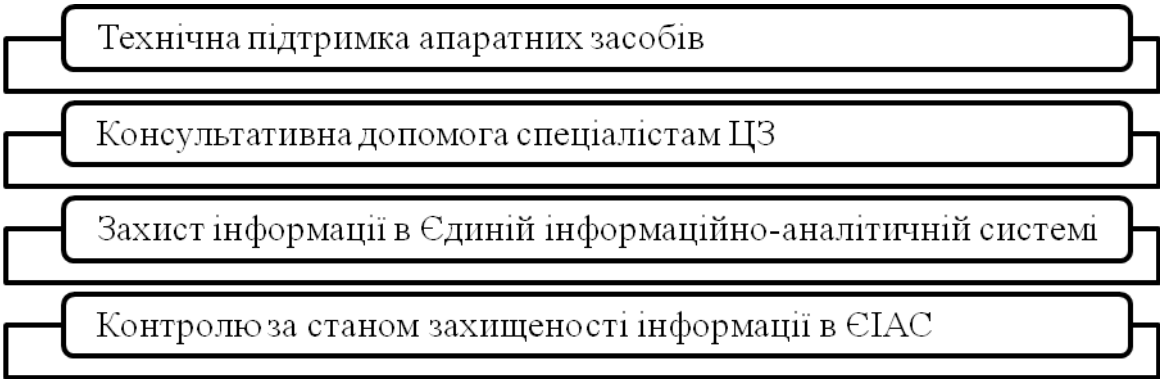

Рисунок 3.1 – Основні завдання відділу інформаційних систем Полтавського обласного центру зайнятості, складено автором за матеріалами установи

Для створення системи захисту документно-інформаційної системи директору Полтавського обласного центру зайнятості слід звернутися до організацій, що мають ліцензію на виконання таких робіт. Виконавцем робіт із створення системи захисту інформації (далі – СЗІ) в інформаційно-телекомунікаційній системі (далі – ІТС) може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право виконання хоча б одного різновиду робіт у сфері технічного захисту інформації (далі – ТЗІ), необхідність проведення якого визначено технічним завданням на створення СЗІ.

Якщо для створення СЗІ Полтавського обласного центру зайнятості необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензію на виконання різновиду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

Створення СЗІ в ІТС Полтавського обласного центру зайнятості здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» на підставі технічного завдання (далі – ТЗ), розробленого згідно з вимогами нормативного документу системи технічного захисту інформації НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на

створення комплексної системи захисту інформації в автоматизованій системі» [33].

До складу СЗІ Полтавського обласного центру зайнятості входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

– витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

– несанкціонованих дій і несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;

– – спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту [33].

Описані загрози подані на рисунку 3.2.

СЗІ спрямована на захист від:	витоку інформації технічними каналами;
	несанкціонованих дій та несанкціонованого доступу до інформації;
	спеціального впливу на інформацію.

Рисунок 3.2 – Основні загрози інформаційній безпеці, які вирішуються у СЗІ Полтавського обласного центру зайнятості, складено автором за [33]

Для кожної ІТС склад, структура і вимоги до СЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи і умовами її експлуатації.

Для формування загальних вимог до СЗІ в ІТС здійснюється обґрунтування необхідності її створення на підставі вимог законодавства, що встановлюють обов'язковість забезпечення конфіденційності, цілісності і доступності інформації, та обстеження середовищ функціонування ІТС – обчислювальної системи, фізичного середовища, середовища користувачів, оброблюваної інформації і технології її обробки.

За результатами детального аналізу об'єкта, на якому створюється СЗІ, уточнення моделі загроз та моделі порушника, результатів аналізу можливості керування ризиками здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій і документальне оформлення політики безпеки.

Технічне завдання на створення СЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС у вигляді окремого розділу ТЗ на створення ІТС, окремого (часткового) ТЗ або доповнення до ТЗ на створення ІТС.

В ТЗ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її обробки в обчислювальній системі ІТС, а також вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою ІТС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Проект СЗІ розробляється на підставі та у відповідності до ТЗ. Під час розробки проекту СЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів СЗІ, а також різних заходів і способів захисту інформації. У результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань і управління СЗІ.

Введення СЗІ в дію включає розробку розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС, створення служби захисту інформації, розробку і затвердження Плану захисту інформації, навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та адміністраторів), комплектування СЗІ засобами захисту інформації, матеріалами, обладнанням, проведення будівельно-монтажних і пусконалагоджувальних робіт, попередніх випробувань і дослідної експлуатації СЗІ.

Під час попередніх випробувань перевіряються працездатність СЗІ та відповідність її вимогам ТЗ. Під час дослідної експлуатації:

– відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

– співробітники служби захисту інформації та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

– здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування комплексу засобів захисту інформації від несанкціонованого доступу;

– здійснюється (за необхідністю) коригування робочої та експлуатаційної документації [33].

Етапи дослідної експлуатації подані на рисунку 3.3. За результатами дослідної експлуатації приймається рішення про готовність СЗІ в ІТС до представлення на державну експертизу.

Для проведення експертизи СЗІ в ІТС або засобу технічного захисту інформації Замовник надсилає заяву встановленої форми на ім’я Голови

Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) [33].

Рисунок 3.3 – Етапи дослідної експлуатації системи захисту інформації Полтавського обласного центру зайнятості, складено автором за [33]

За результатами розгляду заяви у місячний термін приймається рішення про можливість й доцільність проведення експертизи та визначення підрозділу Держспецзв'язку, підприємства, установи або організації, які проводитимуть експертизу. Відносини між Замовником і Організатором експертизи регламентуються укладеним між ними договором про проведення експертизи. Термін проведення експертизи визначається договором і не повинен перевищувати шести місяців. У разі значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації Держспецзв'язку і Замовника.

Замовник надає Організатору експертизи комплект організаційно-технічної документації на СЗІ в ІТС або засіб ТЗІ, необхідний для проведення експертних випробувань. Організатор експертизи, за результатами аналізу наданих Замовником документів і з урахуванням загальних методик оцінювання задекларованих характеристик об'єкта експертизи, формує програму і окремі методики проведення експертизи та розробляє, у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань і відповідне програмно-технічне забезпечення.

Програма проведення експертизи узгоджується із Замовником та Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації Держспецзв'язку, а окремі методики – із зазначеним департаментом.

Терміни розробки окремих методик і необхідного програмно-технічного забезпечення залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи. Результати експертних робіт за окремими методиками оформлюються у вигляді протоколу виконання робіт, затвердженого Організатором експертизи.

У разі виявлення невідповідності об'єкта експертизи вимогам нормативних документів з ТЗІ, Організатор експертизи може запропонувати Замовнику виконати доробку СЗІ в ІТС або засобу ТЗІ. Терміни доробки визначається спільним протоколом або додатковою угодою до договору між Замовником та Організатором експертизи. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.

За результатами проведених робіт Організатор експертизи складає експертний висновок щодо відповідності СЗІ в ІТС або засобу ТЗІ вимогам нормативних документів з ТЗІ і разом з протоколом виконання робіт з подає до Адміністрації Держспецзв'язку. У разі наявності у Замовника обґрунтованих претензій щодо порядку проведення або результатів експертизи, він може звернутися до Адміністрації Держспецзв'язку з пропозицією щодо здійснення контролю за проведенням Організатором експертизи експертних робіт.

Експертний висновок на засіб ТЗІ реєструється і видається Замовнику у разі затвердження результатів експертизи. Зареєстрований Атестат відповідності за підписом Голови (заступника Голови) Держспецзв'язку видається Замовнику на підставі позитивного рішення щодо експертизи СЗІ в ІТС [33].

Видача Замовникам зареєстрованих Експертних висновків про відповідність засобів технічного захисту інформації вимогам нормативних документів з ТЗІ та Атестатів відповідності комплексних систем захисту інформації в

інформаційно-телекомунікаційних системах вимогам нормативних документів з ТЗІ здійснюється безоплатно.

3.2 Вимоги до комплексної системи захисту Єдиної інформаційно-аналітичної системи Служби зайнятості України Полтавського обласного центру зайнятості

Для вдосконалення та побудови системи захисті документно-інформаційних ресурсів Полтавського обласного центру зайнятості важливим етапом є формування вимог до неї, оскільки кожна система має ряд своїх особливостей. Аналізуючи роботу Полтавського обласного центру зайнятості можна сформувати комплекс необхідних дій, що мають бути виконанні при побудові СЗІ.

Опишемо основні вимоги до захисту документно-інформаційної системи Полтавського обласного центру зайнятості, що сформовані у результаті роботи із спеціалістами відділу . У ході виконання робіт з побудови СЗІ ІС виконавець повинен надати ряд послуг, основні групи яких подані на рисунку 3.4.

На першому етапі відбувається Формування загальних вимог до СЗІ. Перш за все проводиться обстеження поточного стану середовищ функціонування ІС. З метою уточнення об’єму побудови СЗІ і створення політики безпеки СЗІ ІС необхідно провести обстеження середовищ функціонування ІС.

Під час проведення обстеження ІС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки.

– У відповідності до НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» під час проведення обстеження середовищ функціонування ІС необхідно провести: обстеження обчислювальних систем

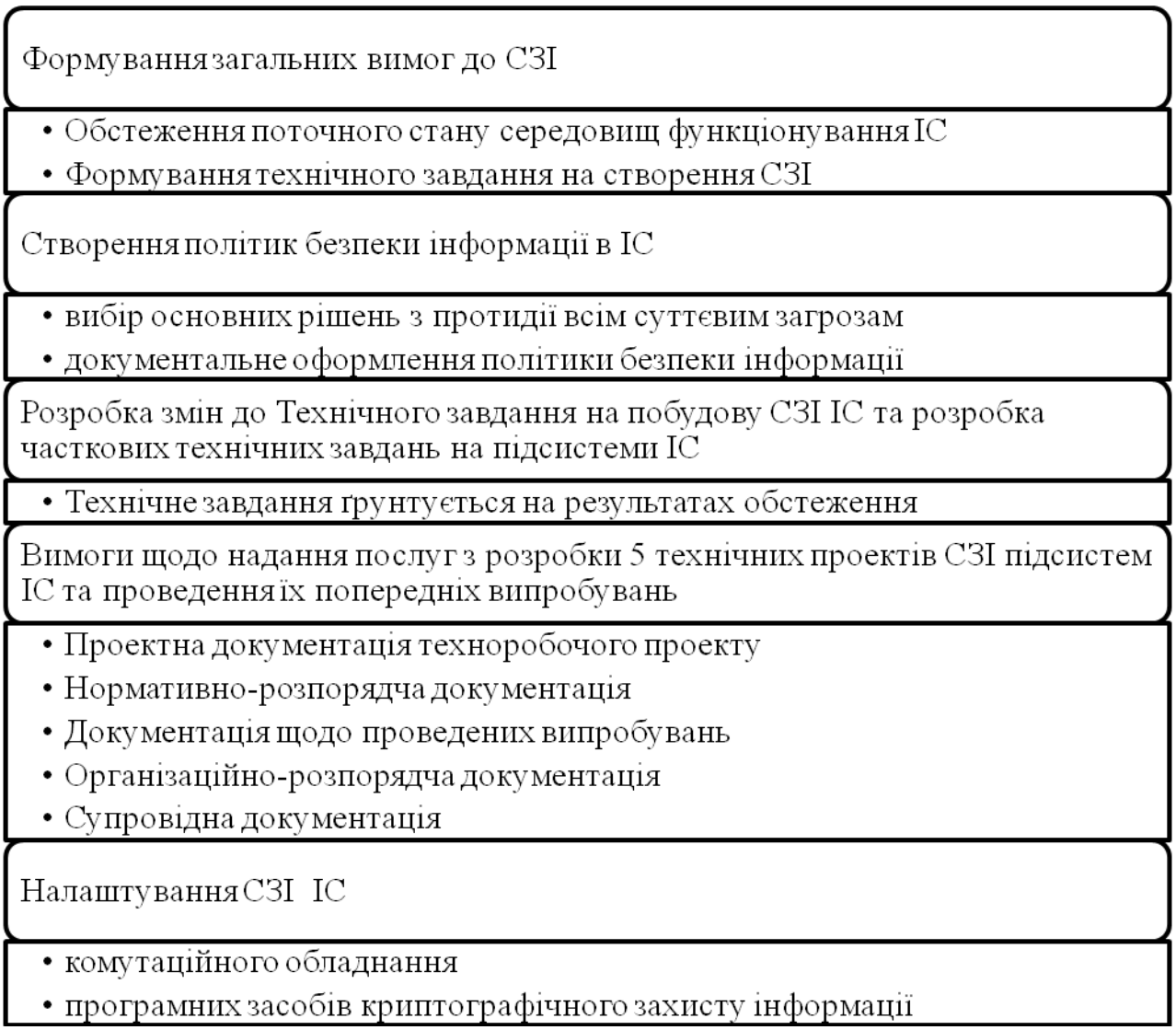

Рисунок 3.4 – Послуги з побудови СЗІ документно-інформаційної системи СЗУ, складено автором за [40]

– ІС; обстеження інформаційного середовища ІС; обстеження фізичного середовища ІС; обстеження середовища користувачів ІС (рисунок 3.5) [33].

За результатами обстеження середовищ функціонування ІС затверджується перелік об’єктів захисту, а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника.

Також необхідно сформувати технічне завдання на створення СЗІ. На цьому етапі:

– визначаються завдання захисту інформації в ІС, мета створення СЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту;

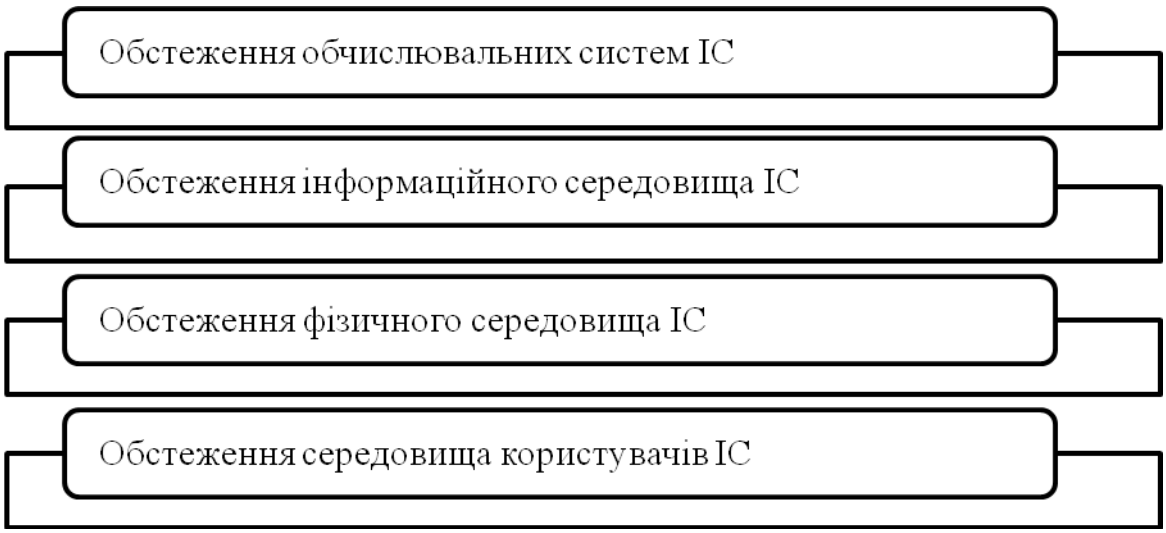

Рисунок 3.5 – Напрями обстеження ІС Полтавського обласного центру зайнятості, складено автором за матеріалами установи

– здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків тощо) і визначається перелік суттєвих загроз;

– визначаються загальна структура та склад СЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів, інші обмеження щодо середовищ функціонування ІС, обмеження щодо використання ресурсів ІС для реалізації задач захисту, припустимі витрати на створення СЗІ, умови створення, введення в дію і функціонування СЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що увійдуть до складу СЗІ.

Складові етапу формування технічного завдання подані на рисунку 3.6.

Після формування технічного завдання переходять до створення політик безпеки інформації в ІС. На цьому етапі здійснюється:

– вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій тощо, які регламентують

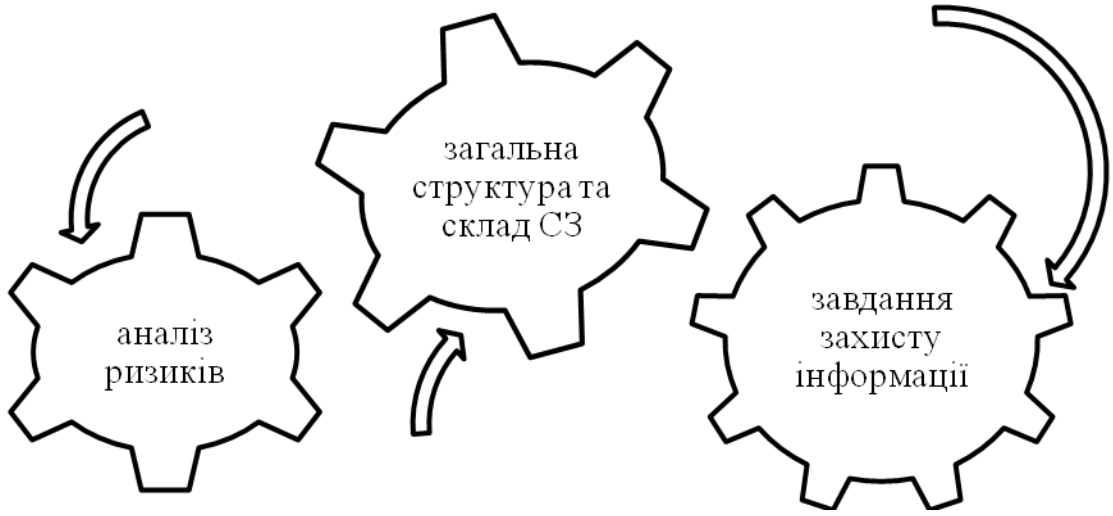

Рисунок 3.6 – Складові етапу формування технічного завдання, складено автором за [40]

використання захищених технологій обробки інформації в ІС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

– документальне оформлення політики безпеки інформації.

– Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001 [33]. Політику безпеки рекомендується оформляти у вигляді окремого документу Плану захисту.

– Після створення політики безпеки відбувається розробка змін до Технічного завдання на побудову СЗІ ІС та розробка часткових технічних завдань на підсистеми ІС. Технічне завдання на СЗІ має бути розроблене з урахуванням вимог НД ТЗІ 3.7-001-99 [33]. Технічне завдання ґрунтується на результатах обстеження.

У зв’язку з тим, що в ІС циркулює інформація з різними рівнями обмеження доступу допускається для окремих підсистем створення часткових технічних завдань на побудову СЗІ відповідної підсистеми.

Інші послуги надаються відповідно до вимог технічних завдань на створення СЗІ ІС, розробленого в рамках проекту та погодженого Адміністрацією Держспецзв’язку України у встановленому порядку.

Технічне завдання повинно містити такі основні підрозділи:

- загальні відомості;

- мета і призначення комплексної системи захисту інформації;
- загальна характеристика автоматизованої системи та умов її функціонування;
- вимоги до комплексної системи захисту інформації;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;
- порядок внесення змін і доповнень до ТЗ;
- порядок проведення випробувань комплексної системи захисту інформації.

При розробці СЗІ висуваються вимоги щодо надання послуг з розробки п’яти технічних проектів СЗІ підсистем ІС та проведення їх попередніх випробувань. У ході надання послуг повинна бути розроблена така документація.

1. Проектна документація технороботочого проекту СЗІ (згідно НД ТЗІ 2.6-001-2011).
2. Нормативно-розпорядча документація СЗІ:

– посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІС (згідно НД ТЗІ 2.6-001-2011):

– інструкція системного адміністратора;

– інструкція адміністратора безпеки.

– технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування СЗІ (згідно НД ТЗІ 2.6-001-2011) [33].

3. Документація щодо проведених випробувань СЗІ:

– програма та методика випробувань СЗІ в ІС (згідно РД 50-34.698-90);

– протокол попередніх випробувань СЗІ в ІС (згідно РД 50-34.698-90) [33].

– Організаційно-розпорядча документація СЗІ: проект наказу про створення СЗІ ІС (згідно НД ТЗІ 3.7-003-99); проект наказу про призначення служби захисту інформації (згідно НД ТЗІ 3.7-003-99); проект наказу про призначення комісії для проведення попередніх випробувань СЗІ ІС (згідно НД ТЗІ 3.7-003-99); проект наказу про створення комісії для приймання СЗІ в дослідну експлуатацію (згідно НД ТЗІ 3.7-003-99) [33]; акт про приймання у

дослідну експлуатацію СЗІ ІС (згідно РД 50-34.698-90) [33]; акт завершення дослідної експлуатації СЗІ ІС (згідно НД ТЗІ 2.6-001-2011); акт завершення робіт зі створення СЗІ в ІС (згідно НД ТЗІ 2.6-001-2011) [33].

– Супровідна документація СЗІ: формуляр (згідно РД 50-34.698-90); реєстраційні журнали, використовувані для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування СЗІ (згідно НД ТЗІ 2.6-001-2011) [33].

Уся проектна документація узагальнено подана на рисунку 3.7.

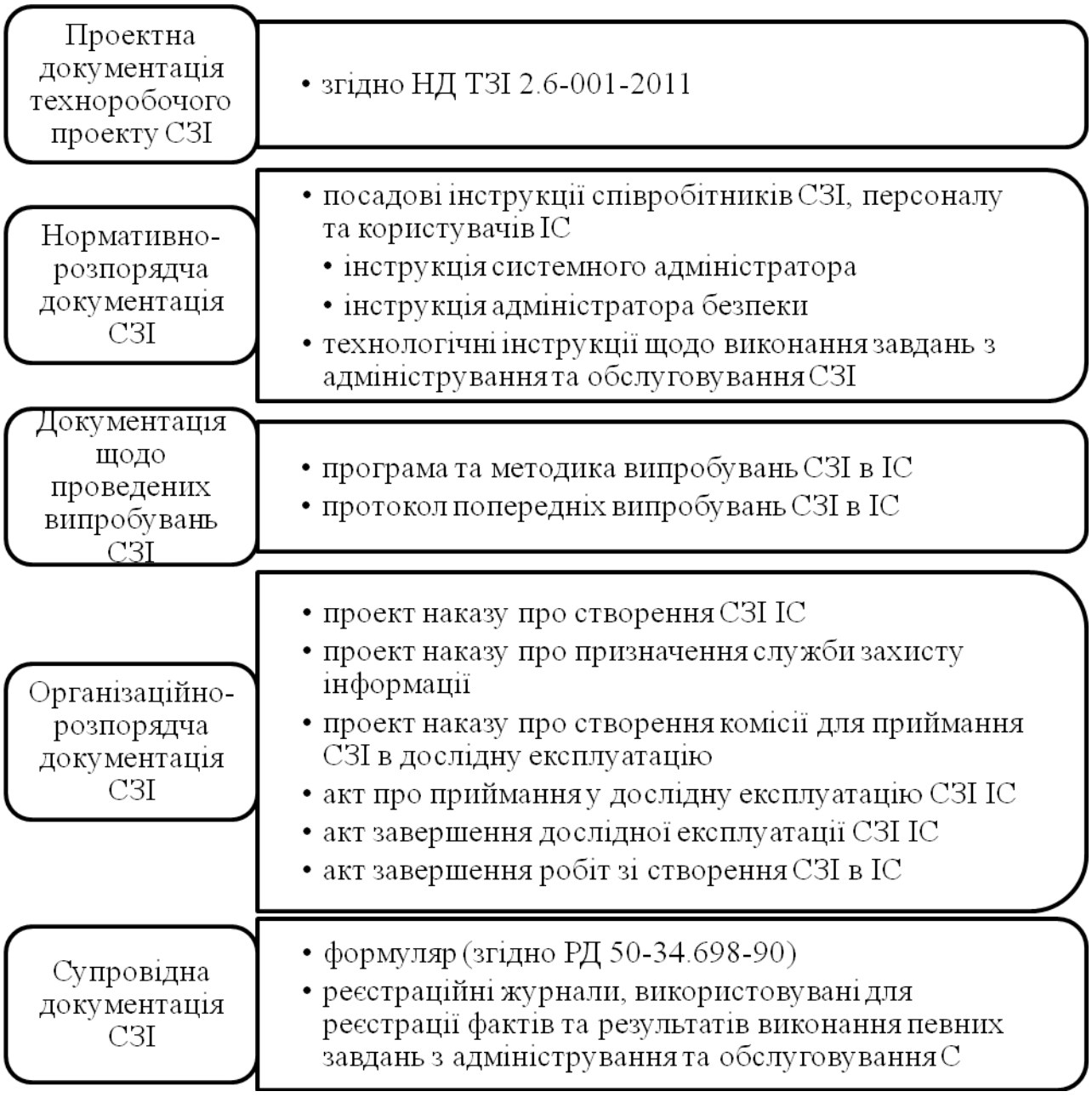

Рисунок 3.7 – Проектна документація при розробці СЗІ, складено автором за [33]

Наступний етап – це налаштування СЗІ ІС Полтавського обласного центру зайнятості. Після створення комплекту технічної документації на СЗІ ІС виконавець повинен виконати роботи з налагодження комплексу засобів захисту СЗІ на території замовника (дослідна ділянка СЗІ ІС), а саме:

- комутаційного обладнання;
- програмних засобів криптографічного захисту інформації.

Дослідна ділянка СЗІ ІС повинна реалізовувати функції криптографічного захисту інформації (що передається по корпоративній мережі державної служби зайнятості між районними, обласними та головним центром (Центральний апарат) від несанкціонованого ознайомлення та/або модифікації.

Засобами криптографічного захисту інформації повинно бути забезпечено резервування та можливість балансування навантаження на компоненти підсистеми криптографічного захисту на Центральному рівні ІТС ДСЗ. Обладнання та засоби КЗІ для дослідної ділянки СЗІ ІС надає Замовник.

Склад комплексу засобів криптографічного захисту інформації поданий на рисунку 3.8.

Рисунок 3.8 – Склад комплексу засобів криптографічного захисту Полтавського обласного центру зайнятості, складено автором за [33]

Опишемо вимоги до кожного із засобів згідно з вимогами установи.

Засіб «Модуль шифрування» (без обмежень на кількість тунелів): повинен бути встановлений на обладнанні в обласному центрі зайнятості; забезпечити

захист трафіку на рівні аутентифікації/шифрування мережевих пакетів за протоколами IPsec AH і / або IPsec ESP; забезпечити пакетну фільтрацію трафіку з використанням інформації в полях заголовків мережевого і транспортного рівнів; забезпечити контекстну фільтрацію для протоколів TCP і FTP; забезпечити класифікацію і маркування трафіку; забезпечити отримання сертифікатів відкритих ключів по протоколу LDAP; забезпечити реалізацію заданого протоколу взаємодії (аутентифікацію та/або захист трафіку) для кожного захищеного з'єднання, доступ в заданому захищеному режимі тільки для зареєстрованих партнерів по взаємодії; забезпечити регульовану стійкість захисту трафіку; забезпечити підтримка NAT Traversal Encapsulation;маскування топології сегмента мережі, що захищається (тунелювання трафіку); забезпечити підтримку списку відкликаних сертифікатів (CRL – Certificate Revocation List); забезпечити реєстрацію подій; забезпечити надання статистики; забезпечити дистанційне та локальне налаштування (за допомогою командної строки або із використанням графічного інтерфейсу).

Засіб «Модуль шифрування (з обмеженням до п'яти тунелів)»: повинен бути встановлений на обладнанні в міських центрах зайнятості; забезпечити захист трафіку на рівні аутентифікації / шифрування мережевих пакетів по протоколах IPsec AH і/або IPsec ESP; забезпечити пакетну фільтрацію трафіку з використанням інформації в полях заголовків мережевого і транспортного рівнів; забезпечити контекстну фільтрацію для протоколів TCP і FTP; забезпечити класифікацію та маркування трафіку; забезпечити отримання сертифікатів відкритих ключів по протоколу LDAP; забезпечити реалізацію заданого протоколу взаємодії (аутентифікацію та/або захист трафіку) для кожного захищеного з'єднання, доступ в заданому захищеному режимі тільки для зареєстрованих партнерів по взаємодії; забезпечити регульовану стійкість захисту трафіку; забезпечити підтримку NAT Traversal Encapsulation; маскування топології сегмента мережі, що захищається (тунелювання трафіку); забезпечити підтримку списку відкликаних сертифікатів (CRL – Certificate

Revocation List); забезпечити реєстрацію подій; забезпечити надання статистики; забезпечити дистанційне і локальне налаштування (за допомогою командної строки або із використанням графічного інтерфейсу).

Засіб «Система керування» повинен забезпечити: можливість відділеного налаштування параметрів функціонування шлюзу; можливість керування списками відкликаних сертифікатів; можливість віддаленої зміни ключових даних; можливість налаштування параметрів системи реєстрації подій; можливість моніторингу стану функціонуючих шлюзів.

Засіб «Центр генерації ключів» повинен забезпечити: керування ключовими даними (генерація закритих, відкритих ключів, формування сертифікату відкритого ключа для інших компонентів; генерація ключових даних безпосередньо для себе; ведення протоколу роботи; ведення та зберігання реєстру ключових даних; архівування реєстру ключових даних; автентифікація адміністратора; перевірки цілісності компонента.

Складові ведення протоколу роботи подані на рисунку 3.9.

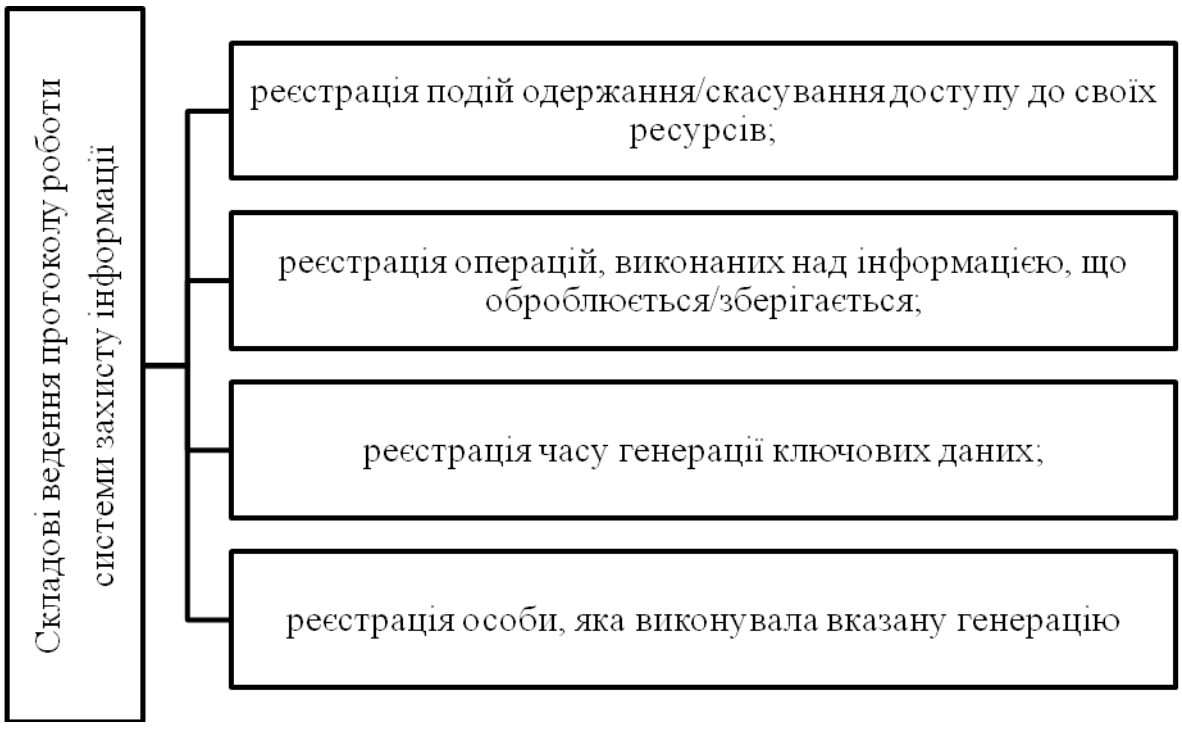

Рисунок 3.9 – Складові ведення протоколу роботи системи захисту інформації, складено автором за [40]

Комплекс повинен реалізувати такі функції (рисунок 3.10):

- захисту даних – забезпечення захисту інформації, яка передається по корпоративній мережі державної служби зайнятості, від несанкціонованого ознайомлення та/або модифікації;
- керування – забезпечення можливості конфігурування та налаштування параметрів компонентів Підсистеми, необхідних для їх функціонування;
- аудиту – забезпечення можливості проводити аналіз записів у файлах протоколів;
- ідентифікації й автентифікації – блокування доступу до можливостей керування підсистемою осіб, що не мають відповідних повноважень;
- захисту функціонування підсистеми від спроб несанкціонованого втручання у її роботу.

Наочно складові комплексу захисту документно-інформаційної системи подані на рисунку 3.10.

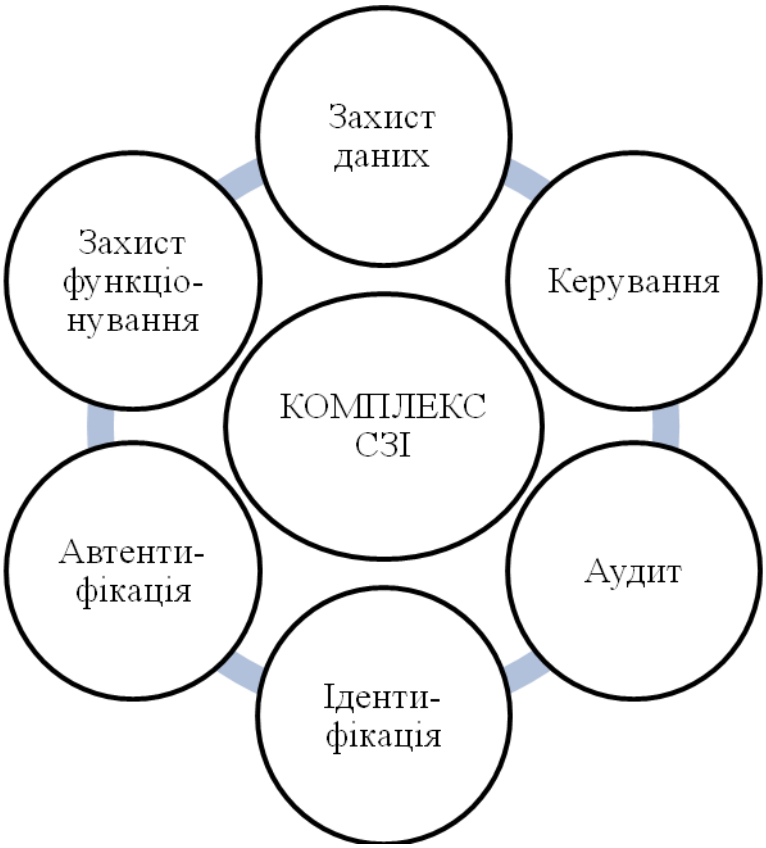

Рисунок 3.10 – Складові комплексу захисту інформації Полтавський обласний центр, складено автором за [33]

Отже, розробка системи захисту документно-інформаціної системи установи – це складне комплексне завдання, яке вирішується із залученням професіональних сертифікованих компаній. Одним із важливих щаблів ефективної реалізації інформаційного захисту є навчання персоналу.

3.3 Проведення тренінгу з інформаційної безпеки як шлях реалізації політики безпеки установи

Одним із шляхів навчання персоналу роботі із системою документно-інформаціного захисту Полтавського обласного центру зайнятості є використання консалтингових послуги з інформаційної безпеки.

Консалтинг інформаційної безпеки – це, перш за все, вид інтелектуальної діяльності. Його основне завдання полягає в аналізі та обґрунтуванні перспектив розвитку, а також у використанні науково-технічних і організаційно-економічних інновацій з урахуванням предметної області і проблем клієнта [47].

Консалтинг в області інформаційної безпеки є комплексом послуг, що надаються компанією-консультантом замовнику з метою визначення: поточного рівня забезпечення (рівня зрілості) інформаційної безпеки в організації, відповідно до найкращих світових практик щодо забезпечення інформаційної безпеки, галузевими вимогами, а також з точки зору ефективності протидії існуючим загрозам інформаційній безпеці; напрямки розвитку інформаційної безпеки, цілей і розв'язуваних задач з урахуванням стратегічних цілей розвитку організації; конкретних дій, необхідних для просування за обраним напрямом і досягнення поставлених цілей і завдань.

Сьогодні консалтинг в області інформаційної безпеки дуже затребуваний на ринку. Це пов'язано з актуальністю завдань, що вирішуються за його

допомогою. Загалом можна виділити чотири основні підстави, які спонукають установи звернутися до консалтингової компанії [56]:

– це відбувається тоді, коли установа не знає, на якому рівні розвитку перебуває інформаційна безпека її ресурсів, чи відповідає вона потребам діяльності і зовнішнім вимогам (законодавство, галузеві, які регулюють вимоги, вимоги замовників і т.п.), немає повного розуміння, які дії необхідно робити і чи потрібні вони взагалі. При цьому в штаті установи відсутні кваліфіковані фахівці, здатні вирішити перераховані вище завдання;

– коли існуюча система інформаційної безпеки побудована і функціонуюча неефективно, і це позначається на поточній діяльності. У такій установі часто виникають інциденти інформаційної безпеки, що призводять до значних збитків, залишаються високі ризики реалізації загроз інформаційній безпеці через відсутність або малу результативність окремих заходів щодо її забезпечення. При цьому в установі не вистачає необхідного досвіду і внутрішніх ресурсів для вибудовування ефективних захисних заходів, а також забезпечення адекватної та своєчасної реакції на виникаючі інциденти інформаційної безпеки;

– коли існує явна необхідність привести наявні механізми забезпечення інформаційної безпеки у відповідність з зовнішніми вимогами в галузі інформаційної безпеки. В основному це відноситься до вимог різних регуляторів в тій галузі, в якій працює установа. Сюди ж можна віднести і виконання вимог законодавства.

– коли організація, досягнувши нового, більш високого рівня розвитку, розуміє, що існуючий рівень забезпечення інформаційної безпеки не тільки не задовольняє поточним потребам, а й є стримуючим фактором для подальшого розвитку. В такому випадку необхідно вибудувати процеси управління інформаційною безпекою, тісно взаємопов'язані з існуючими процесами, що дозволить перевести на вищий щабель розвитку і управління інформаційну безпеку в установі. Це, у свою чергу, допоможе досягти прозорості та ясності питань забезпечення інформаційної безпеки як для вищого керівництва

установи. Такий консалтинг полягає в побудові системи управління інформаційною безпекою відповідно до найкращих світових практик і, при необхідності, у підготовці системи управління до сертифікації за міжнародними стандартами в області інформаційної безпеки.

Існують різні види консалтингу в галузі інформаційної безпеки. Кожен консалтинговий проект в галузі інформаційної безпеки сам по собі унікальний. Однак можна виділити основні види послуг, що надаються консалтинговими компаніями [76]:

- аналітична діяльність (аналіз і оцінка діяльності установи із захисту інформаційних ресурсів, включаючи аналіз ефективності застосовуваних засобів і методів захисту інформації, експертизи проектів, що ведуться в частині інформаційної безпеки, порівняльні дослідження з показниками по галузі та ін.);
- прогнозування (на основі проведеного аналізу і використовуваних консультантом методик – складання прогнозів за вказаними вище напрямками);
- консультації з видачею рекомендацій з найширшого кола питань, що стосуються захисту ресурсів установи, розробки та впровадження заходів і систем захисту;
- стратегічне планування діяльності установи в галузі інформаційної безпеки і рішення сукупності проблем, пов'язаних з організацією управління інформаційною безпекою.

Форми надання послуг також можуть бути різними у залежності від складності проекту і побажань замовника:

- консультації з періодичними виїздами на майданчик замовника для збору вихідних даних, узгодження результатів аналізу і видаються рекомендацій;
- віддалені консультації без виїзду на майданчик замовника;
- постійна присутність на майданчику замовника певного числа консультантів протягом всього терміну проекту (аутстаффінг).

Види та форми консалтингу з інформаційної безпеки подані на рисунку 3.11.

Консалтинг з інформаційної безпеки (кібербезпеки) здійснюється з метою забезпечення безпеки інформаційних систем, активів і приведення їх у відповідність світовим стандартам інформаційної безпеки, таким як ISO 27001, ISA 62443, COBIT 5, NIST SP 800-53 Rev. 4.

Метою приведення у відповідність стандартам інформаційної безпеки є створення умов, які допоможуть контролювати, зберегти і забезпечити цілісність, конфіденційність і доступність інформаційних ресурсів і активів.

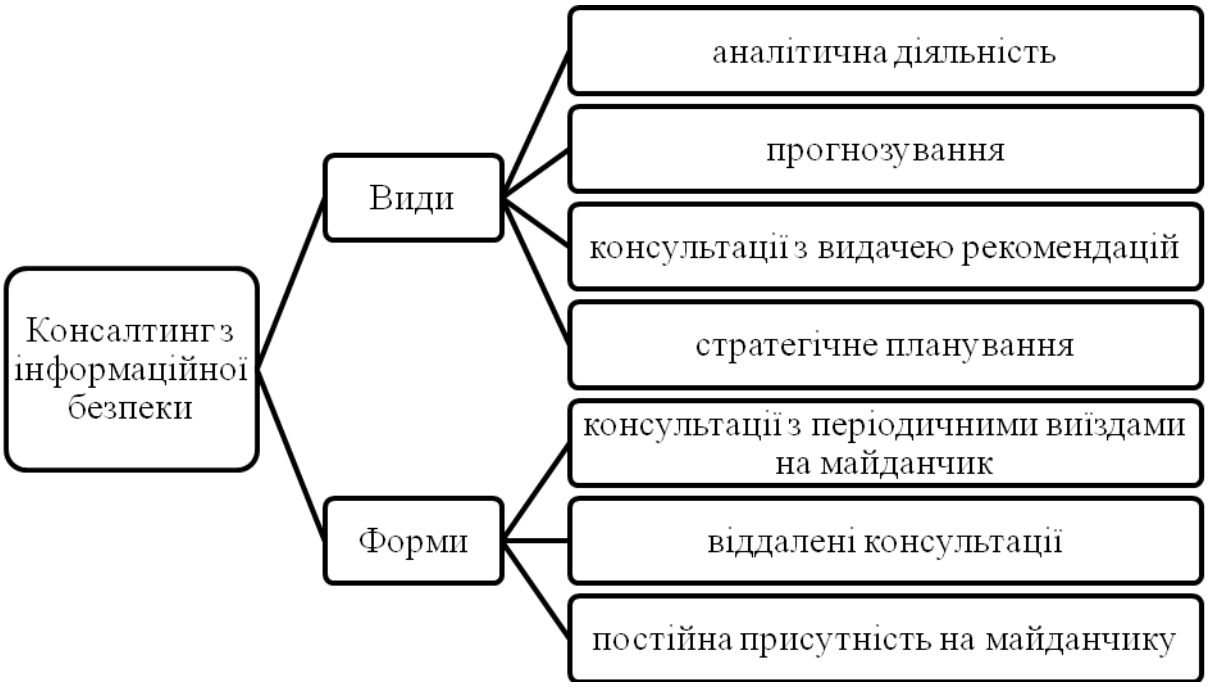

Рисунок 3.11 – Види та форми консалтингу з інформаційної безпеки, складено автором за [75]

Відповідність системи менеджменту інформаційної безпеки світовим стандартам якості дасть такі можливості:

- збільшити продуктивність, завдяки оптимізації діяльності усередині установи;
- економити витрати завдяки захищеності інформації установи і клієнтів, що передбачає відсутність шкоди від інцидентів в галузіі інформаційної безпеки;
- підвищити рівень довіри з боку потенційних клієнтів і партнерів, завдяки прозорості роботи окремих підрозділів і всієї установи в цілому;

- сприятливо відобразиться на іміджі установи в очах клієнтів як потенційних, так і вже існуючих;

Компанії та організації, які мають систему менеджменту відповідно до стандарту ISO 9001, можуть впроваджувати систему менеджменті інформаційної безпеки відповідно до стандарту ISO 27001 з меншою кількістю витрат.

ISO / IEC 27001 – міжнародний стандарт інформаційної безпеки, розроблений Міжнародною організацією зі стандартизації (International Organization for Standardization, ISO) спільно з Міжнародною електротехнічною комісією (International Electrotechnical Commission, IEC), який містить вимоги в області інформаційної безпеки для створення, розвитку та підтримки системи менеджменту інформаційної безпеки. Українським відповідником цього стандарту є ДСТУ ISO/IEC 27001:2015 «Методи захисту системи управління інформаційною безпекою».

Для навчання персоналу Полтавського обласного центру зайнятості можна залучити консалтингові компанії, що надають свої послуги в галузі інформаційної безпеки. Деякі українські компанії подані у таблиці 3.1.

Таблиця 3.1 – Консалтингові компанії, що надають консультації з інформаційної безпеки, складено автором за [73-76]

№ з/п	Назва компанії	Короткий опис послуг в галузі безпеки	Організації-замовники
1.	«Айті-солюшнс»	Аудит, робробка політики, регламентів, правил, впровадження стандартів інформаційної безпеки	«Укрпошта»; «Укртранснафта»; «Укренерго»; «Галавтогаз» та інші.
2.	«ProNet»	Сканування вразливостей мережі; ревізія обладнання; аналіз використовуваного ПО; аналіз інфраструктури на коректність побудови.	«Центр державного земельного кадастру»; ПрАТ «Смарт-холдинг»; ПАО «Запоріжсталь»; ПрАТ «Консюмерс-Скло-Зоря»

Продовження таблиці 3.1

№ з/п	Назва компанії	Короткий опис послуг в галузі безпеки	Організації-замовники
3.	"Соціалізм"	Усі види послуг з інформаційної безпеки. Майстер-класи «Інформаційна безпека» (тривалість 2 тижні)	Компанія «Оболонь», компанія «Космо-Україна», торгівельна марка «Puller», телеканал «Новий Чернігів» та інші.
4.	“Genesis”	Забезпечення безпеки інформаційних систем, активів і приведення їх у відповідність світовим стандартам інформаційної	CMO Веб-студія «Індіго»; CEO Hubber; CEO ТОВ «Хостинг Україна»; Z500 Inter LTD (Польща) та інші.
5.	“BMS-consulting”	Захист даних, захист мереж, аутентифікація та контроль доступу, управління інформаційною безпекою	Телеканал «Україна», ТОВ «Вісті Мас-Медіа», ПрАТ «Сьогодні Мультимедіа», StarLightMedia

Із перелічених компаній лише одна пропонує майтер-клас з інформаційної безпеки ("Соціалізм"). Проте такий захід можуть підготувати та провести спеціалісти відділу інформаційних систем Центру зайнятості.

Для цього необхідно розробити програму тренінгу із захисту документно-інформаційної системи. Тренінгові і традиційні форми навчання мають істотні відмінності. Традиційне навчання здебільшого орієнтоване на правильну відповідь, а тренінг – насамперед, на запитання та пошук. На відміну від традиційних, тренінгові форми навчання повністю охоплюють увесь потенціал людини: рівень та обсяг її компетентності (соціальної, емоційної та інтелектуальної), самостійність, спроможність до ухвалення рішень, взаємодії тощо. Звичайно, традиційна форма передачі знань не є сама собою чимось

негативним, проте у світі стрімких змін і безперервного застарівання знань вона має звужені рамки застосування.

Готуватися до проведення тренінгу для Полтавського обласного центру зайнятості доцільно у три послідовні етапи (рисунок 3.12) – визначити зміст роботи, скласти загальний план проведення занять, детально опрацювати процес ведення тренінгу відповідно до його структури (передбачити, які дії, вправи, рухавки виконуватимуться у відповідній частині заняття).

Рисунок 3.12 – Етапи підготовки тренінгу, складено автором за [47]

Перший етап підготовки – опрацювання змісту тренінгу. Скласти чітке уявлення щодо змісту майбутнього тренінгу допомагає тренеру опрацювання семи важливих питань, які спочатку можна зафіксувати на чернетках. По-перше, слід записати мету тренінгу, тобто те, чого хоче досягти тренер за підсумками всієї роботи, враховуючи потреби учасників.

По-друге, слід уявляти попередній досвід та рівень знань учасників тренінгу. Це дає можливість не лише дати учасникам нову для них інформацію, а й передбачити можливе зіткнення поглядів, яке створюватиме доцільну напругу, що слугуватиме розвитку групової динаміки. По-третє, слід чітко уявляти очікувані результати тренінгу, тобто те, що учасники мають усвідомити або чому навчитися в ході роботи. Тренер коротко занотовує, що зміниться для учасників після проведення тренінгу, формулюючи свої записи так, щоб зрозуміти потенціал для змін.

По-четверте, слід визначити, яким має бути зміст тренінгу, який викладатиметься на тренінгах з тієї чи іншої тематики тобто про що учасникам необхідно дізнатися в процесі навчання. Тренер має опанувати ці матеріали в

повному обсязі, але, плануючи конкретний тренінг, він матиме проблему відбору змістовних матеріалів. Адже їх обсяг досить значний, і обмеження часу тренінгу зазвичай робить неможливим надання всієї відомої інформації. Тому, розробляючи записи щодо змісту певного тренінгу, тренеру доцільно керуватися добрим правилом: запитати себе, про що слухачам абсолютно необхідно дізнатися у зв'язку з даною темою; що було б корисним, але не абсолютно необхідним; про що учасникам було б бажано дізнатися, якби часу було вдосталь. Розподіливши згідно з цим принципом зміст книжок з кожної теми на три блоки, тренер розробляє змістовні матеріали до конкретного тренінгу, і використовує їх залежно від ліміту часу, який виявиться на практиці.

Отже, по-п'яте, потрібно точно знати тривалість тренінгового курсу (півдня, два дні, тиждень тощо). Знання відведеного часу допомагає визначити пріоритети матеріалів змісту тренінгу, певною мірою визначає методи навчання (різні методи потребують різного часу), дає можливість раціонально спланувати тренінг, забезпечуючи достатньо часу на інтелектуальні й рухові вправи, викладання змісту, обговорення роботи, запитання учасників тощо.

Шосте, що необхідно зафіксувати тренеру, готуючись до роботи, – це методи, які застосовуватимуться в ході навчання. Вибір тренером тренінгових методів, технік і технологій їх застосування в кожному конкретному випадку залежатиме з від часових меж, змісту матеріалів, рівня підготовки й характеру взаємин у аудиторії, технічних умов приміщення та обладнання, наявності та якості наочних матеріалів – загалом багатьох чинників, знання й уміння враховувати та ефективно використовувати, які становить невід'ємну частину майстерності тренера.

Насамкінець тренеру слід уважно ознайомитися з майбутнім місцем проведення тренінгу в Полтавському обласному центрі зайнятості: передбачити, як можна змінити розташування столів та стільців; де зможуть працювати малі групи; де можна організувати короткі перерви на кшталт «кава-брейк»; визначити розташування точок електроживлення апаратури, потребу у електроподовжувачах; рівень шуму у приміщенні, можливості регулювання

температури й чистоти повітря тощо – загалом вирішити низку технічних і господарських питань, від яких суттєво залежить успіх тренінгу.

Для підготовки першого етапу доцільно скористатися такою таблицею.

Таблиця 3.2 – Опис першого етапу підготовки тренінгу, складено автором на основі [47]

№	Питання для вивчення	Відповіді
1.	Мета тренінгу	
2.	Попередній досвід учасників	
3.	Очікувані результати тренінгу	
4.	Зміст тренінгу	
5.	Тривалість курсу	
6.	Методи та техніки	
7.	Місце проведення	

Другий етап підготовки – розробка плану проведення занять. План заняття – це документ, який містить інформацію, потрібну тренеру для проведення тренінгу, посібник і ресурсний матеріал, який дає змогу раціонально й організовано провести заняття. Дотримуючись плану, тренер гарантує собі можливість подати доречний матеріал повністю, у логічній послідовності.

Графічно план можна складати в послідовний лінійний спосіб, записуючи всі необхідні пункти один під одним поспіль. Зазвичай цим способом користуються досвідчені тренери, які вже добре знають усі питання, які мають бути відображені у плані.

Інший спосіб, який має певні переваги щодо лінійного планування, полягає у складанні мапи. У таку мапу завжди легше додати ще якийсь пункт, нову ідею, яка оформилася в процесі планування. Цей тип планування графічно імітує те, чим постійно займається наше мислення – встановлення зв'язків між концепціями та емоціями, цілями та перепонами, минулим і теперішнім тощо.

Для того, щоб свої питання щодо проведення тренінгу та відповіді на них записувати на мапі, потрібно заготувати кольорові маркери й великий аркуш 4 паперу, достатній за розміром для фіксування всіх ідей, які виникатимуть у ході планування. У центрі аркуша записуються назва тренінгу, його мета та завдання. Різними кольорами позначаються основні напрями роботи, особливості групи, методи, прийоми та техніки, ресурси, сильні та слабкі сторони ведучого, можливі труднощі, які заважатимуть продуктивній роботі, та дії з їх подолання. Наведений вище перелік семи питань додає теми, які слід відобразити на мапі тренінгу. Колір, величина написів, розмір ліній слугуватимуть позначками важливості означених питань, а стрілки показуватимуть взаємозв'язки між ними. Також можна скористатися програмами створення ментальних карт.

Планування тренінгу – це творчий процес, який потребує чимало часу. Але це надзвичайно корисна робота – у процесі її виконання усвідомлюються нез'ясовані питання, додаються нові, розкриваються перспективи підвищення ефективності тренінгу, які не були відомі раніше. Незалежно від обраної форми, план тренінгу повинен містити певну обов'язкову інформацію.

Текст плану складається із вступу, де мають бути відображені: організація процедури знайомства учасників; господарські питання (розташування місць для коротких перерв, задоволення гігієнічних потреб учасників, порядок використання мобільних телефонів під час занять тощо); загальний огляд тренінгового курсу; загальний огляд першого заняття.

Далі в тексті відображаються зміст заняття та методи, що застосовуватимуться, у тому числі наводяться: докладний опис теми; час, відведений для оцінювання кожної теми; зауваження щодо використання технічних засобів; зауваження щодо використання різних методів навчання; зауваження для тренера щодо певних дій (роздати матеріали, виконати певну вправу тощо).

У тексті плану також відображається порядок підведення підсумків тренінгу, процедури і вправи, що виконуватимуться на завершення роботи. До плану прикладаються додатки, які містять усі необхідні додаткові матеріали тренінгу.

Послідовність розробки плану заняття:

1.Відбір змістовних матеріалів заняття, їх загальний опис у потрібній послідовності.

2.Відбір методів для кожного компоненту заняття.

3.Визначення часу викладання кожного компоненту заняття, установлення часових меж цілісного заняття у загальній тривалості тренінгу.

4.Визначення часових меж перерв, враховуючи, що: для економії часу доцільніше організувати харчування на місці, ніж користуватися відповідними закладами, розташованими в іншому місці; під час тривалих занять у складі малих груп учасникам зручно самим визначати час коротких перерв.

5. Передбачення часу на початку кожного навчального дня для аналізу основних досягнень, відповідей на запитання та пояснення нез'ясованих питань попереднього дня.

6.Передбачення часу наприкінці кожного навчального дня для запитань та зауважень учасників, відповіді на які даватимуться наступного ранку. (Це допомагає контролювати перебіг тренінгових подій.). Передбачення часу наприкінці останнього навчального дня для зведення всіх нез'ясованих питань та надання учасникам можливості завершити оцінювання тренінгу (це забезпечує тренера інформацією про те, які компоненти занять були відпрацьовані ефективно, а які варто поліпшити в майбутньому).

Третій етап підготовки – детальне опрацювання процесу ведення тренінгу відповідно до його структури. Як уже згадувалося раніше, тренінг має досить чітку структуру, частини якої мають визначене змістовне наповнення і рекомендовані часові межі.

На основі проведених досліджень можна скласти алгоритм вдосконалення організації системи безпеки документно-інформаційних ресурсів за рахунок навчання персоналу Полтавського обласного центру зайнятості.

Алгоритм передбачає створення робочої групи або призначення відповідальної особи керівником Полтавського обласного центру зайнятості. Визначення завдань тренінгу для персоналу Полтавського обласного центру зайнятості та категорії персоналу. Пропонуємо тренінг проводити для спеціалістів по обслуговуванню клієнтів Полтавського обласного центру зайнятості, оскільки вони мають доступ до персональних даних.

Основним етапом алгоритму є підготовка та проведення тренінгу. Можливими варіантами є залучення сторонніх спеціалістів, або проведення власними силами, тобто співробітниками відділу інформаційних систем. Оскільки вони знайомі зі специфікою роботи ЦЗ, то за наявності достатнього рівня комунікаційних навичок, це могло б бути кращим та дешевшим варіантом. Алгоритм подано у вигляді ментальної карти на рисунку 3.13, та у вигляді послідовних кроків на рисунку 3.14.

Рисунок 3.13 – Алгоритм вдосконалення системи безпеки документно-інформаційних ресурсів, скриншот ментальної карти, складено автором за результатами дослідження

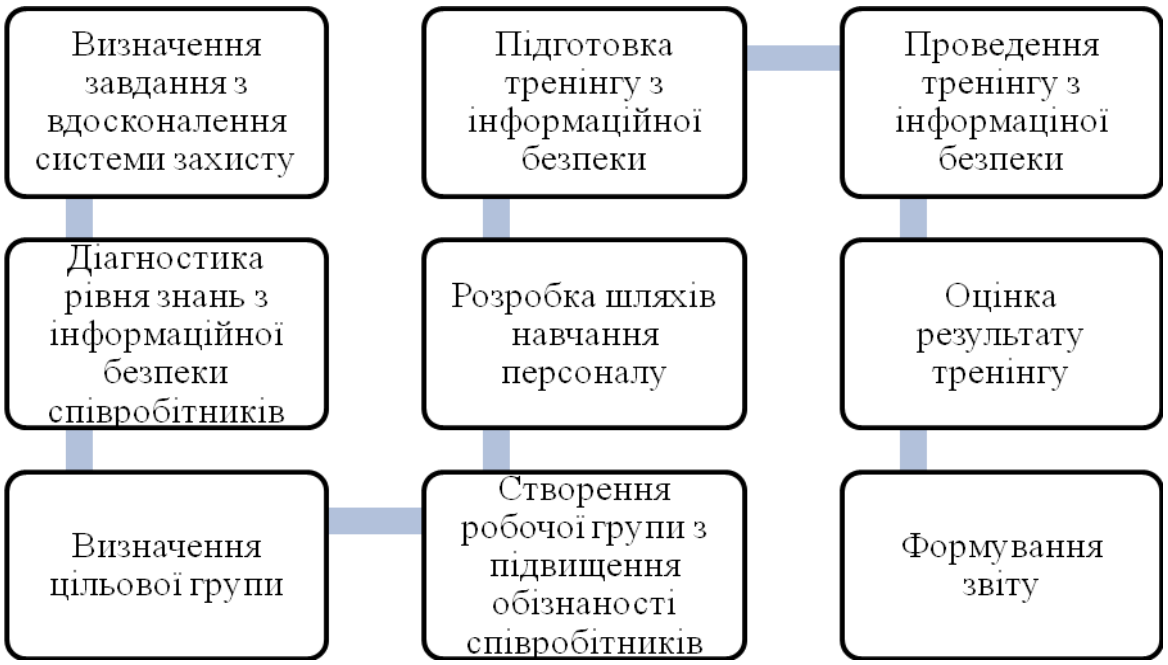

Рисунок 3.14 – Загальний алгоритм вдосконалення системи безпеки документно-інформаційних ресурсів, складено автором за результатами дослідження

Для формування питань, які варто розглянути на тренінгу для спеціалістів з обслуговування населення Полтавського обласного центру зайнятості, пропонуємо використати теоретичний матеріал цього дослідження, а саме пункти 1.2 та 1.3.

Навчання співробітників основам інформаційної безпеки є шляхом покращення організації системи захисту документно-інформаціної системи Полтавського обласного центру зайнятості.

ВИСНОВКИ

У результаті дослідження виконано поставлені завдання та зроблено такі висновки:

1. Визначено теоретичні засади документно-інформаційних систем. Системний характер документних потоків та масивів насправді прямі та зворотні зв’язки з зовнішнім середовищем, які безпосередньо впливають на їх розвиток, отже, документно-інформаційна система потребує захисту своїх ресурсів від загроз різної природи.

2. Досліджено основні поняття інформаційної безпеки та види загроз документно-інформаційній системі установи; У сучасних умовах перед установами гостро постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, що становлять комерційну або державну таємницю. Дії з зовні можуть бути спрямовані на пасивні носії інформації і виражатися, наприклад, в такому: спроби викрадення документів або зняття копій з документів, знімних носіїв;зняття інформації, що виникає на етапі передачі в процесі комунікації; знищення інформації або пошкодження її носіїв;випадкове або навмисне доведення до відома конкурентів документів або матеріалів, що містять комерційну таємницю.

3. Виявлено найпоширеніші методи захисту документно-інформаційних ресурсів установ, що полягає в організації забезпечення захисту. Правове забезпечення – це сукупність законодавчих актів, нормативно-правових документів, положень, інструкцій, вимоги яких є обов’язковими в рамках сфери їх діяльності в системі захисту інформації. Організаційне забезпечення – це гарантування інформаційної безпеки певними структурними одиницями. Інформаційне – це відомості, показники, параметри, що є підставою для вирішення завдань, які забезпечують функціонування системи інформаційної безпеки (показники доступу, обліку, зберігання, різні розрахункові завдання,

пов’язані з діяльністю служби безпеки). Технічне (апаратне) забезпечення передбачає широке використання технічних засобів для захисту інформації та забезпечення діяльності системи інформаційної безпеки. Програмне забезпечення – це різні інформаційні, облікові, статистичні й розрахункові програми, що забезпечують оцінювання наявності й небезпеки різних каналів витоку інформації та способів несанкціонованого доступу до неї. Математичне забезпечення – це математичні методи, які використовують для різних розрахунків, пов’язаних з оцінюванням небезпеки технічних засобів, які мають зловмисники, сфер і норм необхідного захисту. Лінгвістичне забезпечення – це сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері гарантування інформаційної безпеки. Нормативно-методичне забезпечення, що є дотичним з правовим, містить: норми і регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації; різні методики, що забезпечують діяльність користувачів при виконанні своєї роботи за жорстких вимог дотримання конфіденційності.

4. Наведено загальний опис діяльності Полтавського обласного центру зайнятості як підрозділу Державної служби зайнятості, яка створена в грудні 1990 року на підставі постанови Кабінету Міністрів Української РСР від 21.12.1990 № 381 «Про створення державної служби зайнятості в Українській РСР» [32] шляхом перебудови діючої на той час служби працевлаштування на спеціалізовану службу, до завдань якої належить забезпечення комплексного вирішення питань, пов'язаних з регулюванням зайнятості населення, професійною орієнтацією, працевлаштуванням, соціальною підтримкою тимчасово непрацюючих громадян. Основним законодавчим актом, який регулює діяльність державної служби зайнятості, став Закон України «Про зайнятість населення» [11]. Цей закон визначив соціальні гарантії з боку держави в реалізації громадянами права на працю та основні засади діяльності державної служби зайнятості.

5. Проаналізовано Єдину технологія обслуговування незайнятого населення як основа роботи Державної служби зайнятості. Основна мета Єдиної

технології обслуговування незайнятого населення – створення важливого елементу нової адаптованої до умов ринку системи соціального захисту та самозахисту населення; підвищення ефективності роботи державної служби зайнятості щодо надання соціальних послуг безробітним громадянам та роботодавцям. В основу технології покладено дотримання таких принципів організації роботи персоналу як спеціалізація і кооперування праці, пропорційність і синхронність і безперервність. Слід підкреслити, що її кістяк складає набір стандартних матеріальних умов праці і типізованих трудових процесів та організації праці співробітників центрів зайнятості стандартизація і уніфікація форм документації, типізація.

6. Досліджено роботу документно-інформаційної системи «Соціальні послуги та Фонд» Єдиної інформаційно-аналітичної системи державної служби зайнятості. Що стосується послуг, які надаються центрами зайнятості, то вони переважно стандартизовані, а їх організація на місцях здійснюється за принципом уніфікації. Такі досягнення є значними, але найважливішим кроком стали розробка і впровадження Єдиної інформаційно-аналітичної системи (ЄІАС). Це масштабний проект, що немає аналогів в Україні і стосується впровадження сучасних інформаційних технологій у галузі надання послуг населенню. ЄІАС – багатофункціональна система інформаційної підтримки, що забезпечує автоматизацію організаційно-технічних процесів Полтавського обласного центру зайнятості.

7. Визначено порядок створення комплексної системи захисту документно-інформаційних ресурсів. Створення СЗІ в ІТС здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» на підставі технічного завдання, розробленого згідно з вимогами нормативного документу системи технічного захисту інформації НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» [33].

8. Сформульовані вимоги до комплексної системи захисту Єдиної інформаційно-аналітичної системи Служби зайнятості України; Для вдосконалення та побудови системи захисті документно-інформаційних ресурсів важливим етапом є формування вимог до неї, оскільки кожна система має ряд своїх особливостей. Аналізуючи роботу Полтавського центру зайнятості можна сформувати комплекс необхідних дій, що мають бути виконанні при побудові СЗІ. У роботі описані основні вимоги до захисту документно-інформаційної системи Центру зайнятості.

9. Запропонований алгоритм організації тренінгу з інформаційної безпеки як шлях реалізації політики безпеки установи. Консалтинг в області інформаційної безпеки є комплексом послуг, що надаються компанією-консультантом замовнику з метою визначення: поточного рівня забезпечення (рівня зрілості) інформаційної безпеки в організації, відповідно до найкращих світових практик щодо забезпечення інформаційної безпеки, галузевими вимогами, а також з точки зору ефективності протидії існуючим загрозам інформаційній безпеці; напрямки розвитку інформаційної безпеки, цілей і розв'язуваних задач з урахуванням стратегічних цілей розвитку організації; конкретних дій, необхідних для просування за обраним напрямом і досягнення поставлених цілей і завдань.

РЕКОМЕНДАЦІЇ

За результатами дослідження виявлено, що одним із ризиків для безпеки документно-інформаційної системи Полтавського обласного центру зайнятості є недостатня обізнаність персоналу, особливо тих працівників, що мають доступ до інформації, що не має розголошуватись для захисту установи та її клієнтів. З метою зниження цього ризику пропонуємо такі кроки:

1. Визначити завдання з вдосконалення системи захисту Полтавського обласного центру зайнятості, а саме необхідність підвищення рівня знань персоналу з інформаційної безпеки та усвідомленості співробітниками своєї ролі в організації системи захисту установи.

2. Першим кроком є діагностика рівня знань з інформаційної безпеки співробітників Полтавського обласного центру зайнятості, що може бути проведена шляхом усного опитування або тестування.

3. Після діагностики визначити цільову групу, чиї знання з інформаційної безпеки мають невисокі показники, а їх робота пов’язана із персональними даними чи внутрішньою інформацією Полтавського обласного центру зайнятості.

4. Створити робочу групу з підвищення обізнаності співробітників, яка має розробити шляхи навчання персоналу Полтавського обласного центру зайнятості. Пропонуємо підготувати та провести тренінг з інформаційної безпеки. Основні етапи підготовки описані у роботі і можуть бути використані для підготовки тренінгу. У якості теоретичного матеріалу можна використати підрозділи 1.2, 1.3 цього дослідження.

5. Оцінити результату тренінгу, провівши повторне тестування та сформувати відповідний звіт для керівництва Полтавського обласного центру зайнятості.

СПИСОК ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Про бібліотеки і бібліотечну справу [Електронний ресурс] : Закон України від 27.01.1995 № 32/95-ВР Редакція від 01.01.2017 – Режим доступу: https://zakon.rada.gov.ua/laws/main/32/95-%D0%B2%D1%80 (дата звернення : 11.11.2019) – Назва з екрана.

2. Про видавничу справу [Електронний ресурс] : Закон України від 05.06.1997 № 318/97-ВР Редакція від 04.10.2018 – Режим доступу: https://zakon.rada.gov.ua/laws/main/318/97-%D0%B2%D1%80 (дата звернення : 11.11.2019) – Назва з екрана.

3. Про внесення змін до Закону України «Про захист інформації в автоматизованих системах» [Електронний ресурс] : Закон України прийнятий ВРУ 31.05.2005 – Режим доступу: https://zakon.rada.gov.ua/laws/show/2594-15 (дата звернення : 11.11.2019) – Назва з екрана.

4. Про державну таємницю [Електронний ресурс] : Закон України від 21.01.1994 № 3855-XII Редакція від 05.08.2018 – Режим доступу: https://zakon.rada.gov.ua/laws/main/3855-12 (дата звернення : 11.11.2019) – Назва з екрана.

5. Про доступ до публічної інформації [Електронний ресурс] : Закон України від 13.01.2011 № 2939-VI Редакція від 01.05.2015 – Режим доступу: https://zakon.rada.gov.ua/laws/main/2939-17 (дата звернення : 11.11.2019) – Назва з екрана.

6. Про друковані засоби масової інформації (пресу) в Україні [Електронний ресурс] : Закон України від 16.11.1992. Редакція від 04.11.2018 – Режим доступу: https://zakon.rada.gov.ua/laws/main/2782-12 (дата звернення : 11.11.2019) – Назва з екрана.

7. Про електронні довірчі послуги [Електронний ресурс] : Закон України від 05.10.2017 № 2155-VIII – Режим доступу:

https://zakon.rada.gov.ua/laws/main/2155-19 (дата звернення : 11.11.2019) – Назва з екрана.

8. Про електронні документи та електронний документообіг [Електронний ресурс]: Закон України від 22.05.2003 р. № 851-IV. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/851-15 (дата звернення 18.10.2019 р.) – Назва з екрана.

9. Про Єдину інформаційно-аналітичну систему управління соціальною підтримкою населення України (E-SOCIAL) [Електронний ресурс] : Постанова Кабінету Міністрів України від 17 липня 2019 р. № 676 – Режим доступу: https://www.kmu.gov.ua/npas/pro-yedinu-informacijno-analitichnu-sistemu-upravlinnya-socialnoyu-pidtrimkoyu-naselennya-t170719 (дата звернення : 11.11.2019) – Назва з екрана.

10. Про загальнообов'язкове державне соціальне страхування на випадок безробіття [Електронний ресурс] : Закону України (№ 1533-III від 02.03.2000) Редакція від 09.08.2019 – Режим доступу: https://zakon.rada.gov.ua/ laws/show/1533-14 (дата звернення : 11.11.2019) – Назва з екрана.

11. Про зайнятість населення [Електронний ресурс] : Закон України № 803-XII від 01.03.1991. Редакція від 09.08.2019 – Режим доступу: https://zakon.rada.gov.ua/laws/show/5067-17 (дата звернення : 11.11.2019) – Назва з екрана.

12. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 05.07.1994 № 80/94-ВР Редакція від 19.04.2014 – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення : 11.11.2019) – Назва з екрана.

13. Про захист персональних даних [Електронний ресурс] : Закон України від 01.06.2010 № 2297-VI Редакція від 30.01.2018 – Режим доступу: https://zakon.rada.gov.ua/laws/main/2297-17 (дата звернення : 11.11.2019) – Назва з екрана.

14. Про інформацію [Електронний ресурс] Закон України. Прийнятий ВРУ від 2 січня 2010р. Редакція від 01.01.2017 – Режим доступу:

https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 09.11.2019) – Назва з екрана.

15. Про науково-технічну інформацію [Електронний ресурс] : Закон України від 25.06.1993 № 3322-XII Редакція від 19.04.2014 – Режим доступу: https://zakon.rada.gov.ua/laws/main/3322-12 (дата звернення : 11.11.2019) – Назва з екрана.

16. Про Національний архівний фонд та архівні установи [Електронний ресурс] : Закон України від 24.12.1993 № 3814-XII Редакція від 21.05.2015 – Режим доступу: https://zakon.rada.gov.ua/laws/show/3814-12 (дата звернення : 11.11.2019) – Назва з екрана.

17. Про обов'язковий примірник документів [Електронний ресурс] : Закон України від 09.04.1999 № 595-XIV Редакція від 13.01.2016 – Режим доступу: https://zakon.rada.gov.ua/laws/show/595-14 (дата звернення : 11.11.2019) – Назва з екрана.

18. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки [Електронний ресурс] : Закон України прийнятий ВРУ 09.01.2007 - Режим доступу : https://zakon.rada.gov.ua/laws/show/537-16. (дата звернення: 10.10.2019) Назва з екрана.

19. Про створення державної служби зайнятості в Українській РСР [Електронний ресурс] : Постанова КМУ № 381 від 21.12.1990 – Режим доступу: https://zakon.rada.gov.ua/laws/show/381-90-%D0%BF (дата звернення : 11.11.2019) – Назва з екрана.

20. Про організаційні заходи щодо запровадження загальнообов’язкового державного соціального страхування на випадок безробіття [Електронний ресурс] : Постанова Кабінету Міністрів України від 14 червня 2000 року № 955 – Режим доступу: https://zakon.rada.gov.ua/laws/show/955-2000-%D0%BF_(дата звернення : 11.11.2019) – Назва з екрана.

21. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім

електронних довірчих послуг) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації [Електронний ресурс] : Постанова КМУ – Режим доступу: https://zakon.rada.gov.ua/laws/show/915-2018-п. (дата звернення: 15.11.2019) - Назва з екрана.

22. Аніловська Ганна Ярославівна. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. [Електронний ресурс]. - Режим доступу: http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf. (дата звернення: 15.11.2018) – Назва з екрана.

23. Безверхий К.В. Організація та методика електронного документообігу на підприємстві: стан та перспективи розвитку / К. В. Безверхий // Економічна стратегія і перспективи розвитку сфери торгівлі та послуг. – 2013. – Вип. 1(2). – С. 16-25. – [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/esprstp_2013_1(2)__5 (дата звернення : 11.11.2019) – Назва з екрана.

24. Бражко О. В. Розвиток державної політики щодо регулювання ринку праці та управління трудовими ресурсами / О. В. Бражко //Економіка та держава: Державне управління. – 2010. – №2. – С. 103 – 105.

25. Величкевич М.Б. Електронний документообіг, тенденції та перспективи / М.Б Величкевич., Н.В. Мітрофан, Н.Е. Кунанець// Lviv Polytechnic National University Institutional Repository. – 2010. [Електронний ресурс]. Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/20146/1/7-44-53.pdf (дата звернення : 11.11.2019). – Назва з екрана.

26. Виноградова Ганна Валеріївна. Правове регулювання інформаційних відносин в Україні: Навч. посіб. – Київ : Юстініан, 2006. – 171 с.

27. Войнаренко М.П. Інформаційні системи і технології в управлінні організацією / М.П. Войнаренко, О.М. Кузьміна, Т.В. Янчук. Навч. посіб. – Вінниця: ПП Едельвейс і К, 2015. – 496 с.

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

29. Герасимчук В.І. Інновації як фактор економічного розвитку і трансформації зайнятості / В.І. Герасимчук // Регіональні аспекти розвитку і розміщення продуктивних сил України: зб. наук. пр. кафедри управління трудовими ресурсами і розміщення продуктивних сил ТАНГ. – Тернопіль: Економічна думка, 2007. - Вип. 6. – С. 100 – 106.

30. Гриджук Г.С. Систематизація методів інформаційної безпеки підпримства. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf. (дата звернення: 15.11.2019) - Назва з екрана.

31. Група підсистем «Соціальні послуги та Фонд» Єдиної інформаційно-аналітичної системи державної служби зайнятості https://iqusion.com/%D0%B3%D1%80%D1%83%D0%BF%D0%B0-%D0%BF%D1%96%D0%B4%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC-%D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D1%96-%D0%BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3%D0%B8-%D1%82/

32. Державна служба зайнятості [Електронний ресурс] : Офіційний сайт. – Режим доступу: https://www.dcz.gov.ua/ (дата звернення : 11.11.2019) – Назва з екрана.

33. Державна служба спеціального зв’язку та захисту інформації України [Електронний ресурс] : Офіційний сайт. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/ control/uk/index (дата звернення: 15.11.2019) – Назва з екрана.

34. Документ та документаційне забезпечення управління в Україні. Сайт «Государство для общества» [Електронний ресурс]. – Режим доступу: http://www.govforc.com/index.php?id=265 (дата звернення : 11.11.2019) – Назва з екрана.

35. Е-будущее информационное право / В. М. Брыжко, А. Л. Орехов, О. Л. Гальченко [и др.]; Под ред. Р. А. Калюжного, М. Я. Швеца. – Киев: Интеграл, 2002. – 264 с.

36. Закрите акціонерне товариство «Софтлайн» : Єдина інформаційно-аналітична система Служби зайнятості України [Електронний ресурс] : – Режим доступу: http://krashiy.com/rus/nominations2006/?nid=17&id=30 280&pid=242 (дата звернення : 11.11.2019) – Назва з екрана.

37. Захист інформаційних систем – важливе завдання сьогодення [Електронний ресурс] : – Режим доступу : http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/ – Назва з екрана. – Дата звернення : 20.09.19.

38. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. / В.М. Брижко, О.М. Гальченко, В.С. Цимбалюк [та ін.] – Київ : Інтеграл, 2002. – 220 с.

39. Інформаційний перелік документів Фонду нормативних документів у сфері технічного та криптографічного захисту інформації. [Електронний ресурс] : – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=89740&cat_id=89734&ctime=1547204009788_(дата звернення : 11.11.2019) – Назва з екрана.

40. Інформація [Електронний ресурс] : сайт про інформацію – Режим доступу: https://uk.wikipedia.org/wiki/Інформація. (дата звернення: 15.11.2019) – Назва з екрана.

41. Коростельов В.А. Управлінське консультування: навч. посібник / В.А. Коростельов. – Київ : МАУП, 2013. – 104 с.

42. Короткий курс лекцій з дисципліни «Інформаційні системи і технології в економіці і управлінні» [Електронний ресурс] – Режим доступу: http://studme.com.ua/158407208766/informatika/informatsionnye_sistemy_i_tehnologii_v_ekonomike_i_upravlenii.htm (дата звернення: 15.11.2019) – Назва з екрана.

43. Кропивко М.Ф. Організація інформаційно-консультаційної діяльності:навчальний посібник / М.Ф. Кропивко, Т.П. Кальна-Дубінюк, М.Ф. Безкровний. – Москва : Агроконсалт, 2004. – 348с.

44. Курбан О. В. Основи сучасної національної інформаційної безпеки України / О. В. Курбан // «Вісник Харківської державної академії культури» Серія: Соціальні комунікації. – 2017, Випуск 50.– С. 55-66.

45. Лєсовець Н.М. Документаційне забезпечення управління: проблеми та перспективи/ Н.М. Лєсовець / Педагогіка – Вісник Луганського національного університету імені Тараса Шевченка.[Електронний ресурс]. Режим доступу: http://www.stattionline.org.ua/pedagog/104/18285-dokumentacijnezabezpechennya-upravlinnya-problemi-j-perspektivi.html (дата звернення : 11.11.2019) – Назва з екрана.

46. Литвинова Н.Н. Кто заплатит сверхурочные термину документ? / Н.Н. Литвинова // Науч. и техн. б-ки. – 2007. – № 9. – С. 62

47. Лісіна С.О. Документні ресурси: навч. посібник / С.О. Лісіна. – Львів: Видавництво Львівської політехніки, 2013. – 240 с.

48. Маршавін Ю.М. Єдина технологія надання соціальних послуг [Електронний ресурс] : Науково-дослідна робота / [Ю.М. Маршавін, Л.М. Фокас, Л.Є.Ляміна, Д.Ю. Маршавін]. – Київ –2010 – Режим доступу: http://ipk.edu.ua/etnasp/ (дата звернення : 11.11.2019) – Назва з екрана.

49. Нормативне забезпечення інформаційної безпеки: Підручник / С.М. Головань, О.С. Петров, В.О. Хорошко [та ін.]; За ред. проф. В.О. Хорошка. – Київ: ДУІКТ, 2008. – 533 с.

50. Ортинський В.Л. Економічна безпека підприємств, організацій та установ: навч. посібник / В.Л. Ортинський, І.С. Керницький, З.Б. Живко. – Київ : Правова єдність, 2009. – 542 с.

51. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] : / В. Петрик // Юридичний журнал. – 2009. – № 5. – Режим доступу : https://web.archive.org/web/20150710023330/http://www.justinian.com.ua/article.php?id=3222 – Назва з екрана. – Дата звернення : 22.09.19.

52. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : Затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. N 373. – Режим доступу : https://www.kmu.gov.ua/ua/npas/32791826. – Назва з екрана. – Дата звернення : 19.09.19.

53. Саввіна Л.І. Комунікація як чинник розвитку суспільства / Л.Саввіна. – Одеса, 2004. – 234 с.

54. Світлична В.Ю. Забезпечення інформаційної безпеки банківських установ / В.Ю. Світлична // Крымский экономический вестник: Научный журнал. №1 (08) лютий 2014. Частина ІІ. – Сімферополь, 2014. – С.172-175.

55. Северинов А.В. Анализ угроз и рисков безопасности информации в беспроводных сетях / А.В. Северинов, В.И. Черныш // Системи управління, навігації та зв'язку. – Вип. 1. – К.: ЦНДІ НіУ, 2011. – С. 229–232.

56. Сєвєрінов О.В. Управління інформаційною безпекою згідно міжнародних стандартів / О.В. Сєвєрінов, В.І. Черниш, М.Є. Молчанова // Системи управління, навігації та зв'язку. – Вип. 4. – Київ : ЦНДІ НіУ, 2011. – С. 250–253.

57. Системи менеджменту інформаційної безпеки: Навч. посібник / В. А. Ромака, В. Б. Дудикевич, Ю. Р. Гарасим [та ін.] – Львів: Львівська політехніка, 2012. – 232 с.

58. Славко І. О. Безпека документно-інформаційної системи установи / І. О. Славко, М. В. Макарова // Збірник наукових статей магістрів. Інституту економіки, управління та інформаційних технологій. – Полтава : ПУЕТ, 2019. – Ч. 1. – С. 36-41

59. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи. [Електронний ресурс]. / О. А. Сороківська, В. Л. Гевко – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf. (дата звернення: 15.11.2019) – Назва з екрана.

60. Сучасне діловодство: зразки документів, діловий етикет, інформація для ділової людини/ ред. : В.М. Бріцина. – Київ : Довіра, 2007. – 687 с.

61. Сучасне діловодство: сутність, особливості, структура [Електронний ресурс] – Режим доступу: https://paholok.io.ua/s1193335/suchasne_dilovodstvo_sutnist_osoblivosti_struktura (дата звернення 10.05.2019) – Назва з екрана.

62. Твердохліб М.Г. Інформаційне забезпечення менеджменту: Навчальний посібник / М.Г. Твердохліб. – Київ: КНЕУ, 2002. – 224с.

63. Теоретичні аспекти інформаційно-документаційного забезпечення організації [Електронний ресурс] – Режим доступу: https://sites.google.com/site/informacijnodokumentacijne/teoreticni-aspekti-informacijno-dokumentacijnogo-zabezpecenna-organizaciie (дата звернення 10.05.2019) – Назва з екрана.

64. Терещенко Л.О. Інформаційні технології в управлінні / Л.О. Терещенко, О.С. Сніжко // Інвестиції: практика та досвід. – 2011. – № 12. – С. 28–31.

65. Товт І.С. Загальна характеристика документних потоків та масивів у системі докуметних комунікацій [Електронний ресурс] : // І.С. Товт, К.Ф. Трохимчук – Режим доступу: http://dspace.tneu.edu.ua/bitstream/316497/11412/1/%D0%A2%D0%BE%D0%B2%D1%82.pdf_(дата звернення: 15.11.2019) – Назва з екрана.

66. Управління документообігом [Електронний ресурс] – Режим доступу: https://www.osgrm.ua/poslugy/upravlinnya-dokumentoobigom/ (дата звернення 10.01.2019) – Назва з екрана.

67. Федоренко В.Г. Державна служба зайнятості України в контексті протидії новим викликам ринку праці / В.Г. Федоренко // Економіка та держава: Економічна наука. – 2009. – № 11. – С. 83 – 85.

68. Федоренко В.Г. Діяльність державної служби зайнятості в ринкових умовах / В.Г. Федоренко // Економіка та держава: Актуально. – 2009. – № 10. – С. 4 – 5.

69. Філіпова Л.Я. Системи управління електронним документообігом: загальні поняття термінології, організації, технології (зарубіжний досвід) / Л.Я. Філіпова // Вісник Книжкової палати України. –2001. – № 4. – С. 15–18.

70. Хілінський А. Електронний цифровий підпис (у запитаннях і відповідях) [Електронний ресурс]. / А. Хілінський // Секретарь-референт. – № 1, – 2011 Режим доступу: http://www.trainings.ua/article/2113.html (дата звернення : 11.11.2019) – Назва з екрана.

71. Швецова-Водка Г.М. Документознавство / Г. М. Швецова-Водка – Київ, 2007. – 398 с.

72. Юркова Д. Ю. Діяльність Державної служби зайнятості в умовах ринкової системи [Електронний ресурс] : / Д. Ю. Юркова, С. Ю. Ганус //Економічні науки, №5. Управління трудовими ресурсами – Режим доступу: http://www.rusnauka.com/14_NPRT_2010/Economics/66813.doc.htm (дата звернення: 15.11.2019) – Назва з екрана.

73. Genesis [Електронний ресурс] : Офіційний сайт компанії. – Режим доступу: http://genesis-legal.com/ (дата звернення: 15.11.2019) – Назва з екрана.

74. IT-Solutions [Електронний ресурс] : Офіційний сайт компанії. – Режим доступу: https://it-solutions.ua/ (дата звернення: 15.11.2019) – Назва з екрана.

75. ProNet [Електронний ресурс] : Офіційний сайт компанії. – Режим доступу: https://pronet.ua/ (дата звернення: 15.11.2019) – Назва з екрана.

76. Socialism [Електронний ресурс] : Офіційний сайт компанії. – Режим доступу: https://socialism.com.ua/ua/(дата звернення: 15.11.2019) – Назва з екрана.