Бобошко М.

Перелік скорочень

ОІД – об’єкт інформаційної діяльності

АС - автоматизована система

НПА – нормативно-правова база

ТЗІ – технічний захист інформації

ІБ – інформаційна безпека

ПО – програмне забезпечення

ПК – персональний компьютер

НСД – несанкціонований доступ

ЕВМ – електронно обчислювальна техніка

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Стан питання

Ні для кого не є секретом, що інформаційні технології сьогодні правлять світом. Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, підприємства, держави. Сьогодні ми все більше й більше використовуємо їх у своїй діяльності. Але взявши на службу телекомунікації і глобальні комп'ютерні мережі, слід знати й розуміти, які можливості для зловживання створюють ці технології. Сьогодні жертвами хакерів можуть стати не лише підприємства, але й цілі держави.
Щоб не бути голослівним, можна поглянути на статистику кібератак за останні декілька років:

1. **6 грудня 2016 року** хакерська атака на урядові сайти (Держказначейства України та інших) і на внутрішні мережі держорганів призвела до масштабних затримок бюджетних виплат.
2. **17-18 грудня 2016 року** Електроенергія була відсутня протягом 1 години 15 хвилин. Вимкнено струм у північній частині Києва на правому березі і частині прилеглих районів Київської області
3. **14 квітня 2017 року** з'явилось перше відоме оновлення програми M.E.Doc уражене бекдором. Завдяки йому 18 травня 2017 року сталась перша масова кібератака вірусом XData. 27 червня 2017 року сталась друга масштабна хакерська атака хробаком-винищувачем NotPetya, яка вразила майже 80 % підприємств в Україні а також перекинулась на підприємства закордоном. Бекдор тривалий час дозволяв зловмисникам викрадати інформацію з підприємств та відкривав доступ зловмисникам до комп'ютерних мереж.

Тому кібербезпека — одна з основних проблем, що викликає занепокоєння. І чим швидше людство розвиває інформаційні технології, тим більшою

є потреба в захисті інформаційно-телекомунікаційних систем. Оскільки критичні вразливості в програмному забезпеченні та автоматизованих системах викликають небезпідставні побоювання, то не дивно, що уряди та суспільство в усьому світі шукають кращих заходів і методів для захисту особистих даних Інтернет-ресурсів від кіберзагроз.

Але незважаючи на суттєві переваги прогресу не всі підприємства квапляться впроваджувати їх у робочий процес. Наприклад, державні підприємства, здебільшого мають консервативний погляд на інновації. Оскільки дуже важко оцінити з першого погляду, що великі витрати на те що не принесе прибутку одразу може принести його у довготривалій перспективі.

Так деякі державні установи ще якихось 5 років тому мали паперовий документообіг і вважали електронний реєстр безглуздою забаганкою. Але час і потреби постійно змінюються. З'являються нові підприємства, а старі зникають бо не змогли пристосуватися до мінливості середовища. Але не всі підприємства мають за головну ціль отримати прибуток. Є так звані ентузіасти, що мають на меті покращення життя для себе та людей, що проживають поруч. Іванов І. І. у 1999 р. мав мрію залучити кошти для розбудови та покращення міста у якому народився та жив 47років.

Так в 2000 році з'явилось державне підприємство під назвою «Інвестиційний центр». Спочатку у своєму штаті підприємство мало трьох чоловік: Засновника(Директора), Бухгалтера та Юриста. Маючи широкий спектр послуг підприємство не бажало полегшити та автоматизувати працю своїх робітників. Але в 2008 р. змінився керівник підприємства та вніс великі зміни. Він розширив штат, змінив назву підприємства на «Інвестиційно-інноваційний центр» та обрав провідні галузі для подальшої праці. Оновлене підприємство зіштовхнулось із певними проблемами в зв'язку із розширенням штату. Так довелось змінити офіс і обрати нові шляхи забезпечення фізичного захисту. Виявилося, що зберігати, оформлювати, а тим паче швидко знаходити необхідну інформацію в цілком паперовій документації це дуже велика проблема. Тому 2010 рік можна вважати

початком становлення автоматизованої системи даного підприємства. Саме в цьому році була створена база даних та локальна мережа, що поєднала усіх працівників ІІЦ. Із плином часу вдосконалювалась система, так з'явився інтернет сайт, нові бази даних. Зав'язались партнерські стосунки зі схожими підприємствами, з'явились конкуренти на ринку. Оскільки системи Інтернет комунікацій були налаштовані лише один раз в момент їх створення або за допомогою запрошених людей. Не маючи належного супроводу та налаштована так «аби працювало» В 2018 році фірма втратила майже всю напрацьовану інформацію через ураження системи вірусом Yatron Ransomware. Після цього інциденту стало зрозуміло, що подальше існування підприємства без створення захищеної системи обробки інформації та управління інформаційною безпекою неможливе.

1.1.1 Інформаційна безпека у інвестиційному бізнесі

За умов конкурентного середовища значного поширення набули такі негативні явища, як підслуховування, викрадення конфіденційної інформації на матеріально-речових носіях, зняття інформації з технічних каналів через комп'ютерні мережі. На сьогодні інформаційна безпека дедалі більше стосується саме суб'єктів підприємницької діяльності, яким потрібно захищатися від відтоку інформації. Інформаційна безпека — це здатність персоналу підприємства забезпечити захист інформаційних ресурсів та потоків від загроз несанкціонованого доступу до них. За результатами негативного впливу на основні властивості інформації (конфіденційність, цілісність, доступність) вирізняють дестабілізуючі фактори техногенного, антропогенного, природного характеру. Останнім часом розвиток суспільства характеризується негативною динамікою не тільки зловмисних порушень роботи інформаційних систем чи мереж, а й злочинів, вчинених з використанням новітніх технологій, найсучаснішої техніки.

Деякі керівники комерційних структур у своїй підприємницькій діяльності не приділяють належної уваги інформаційній безпеці підприємства, що дозволяє зловмиснику використовувати недоліки захисту інформаційних автоматизованих систем й обчислювальної техніки. Одним із шляхів усунення цих недоліків у сфері підприємництва є проектування організаційно-функціональної підсистеми інформаційної безпеки підприємства і її ресурсного забезпечення. Сфера інформаційної безпеки потребує оцінювати вчинки зловмисників, які модифікують, знищують або сприяють крадіжці інформації. Виходячи з аналізу конкретної ситуації, а також технології обробки та захисту даних в інформаційних системах, враховуючи засоби і методи негласного зняття інформації, це роблять порушники правового режиму безпеки інформації. Актуальність досліджуваної проблеми полягає в тому, що з розвитком конкуренції значного поширення набули такі злочини, як викрадання інформації через комп'ютерні мережі і прослуховування ліній зв'язку. Тому знання потенційних загроз, причин та умов скоєння таких злочинів дозволить працівникам підрозділів служб безпеки підприємств у межах своєї компетенції здійснити заходи, що стануть перешкодою на шляху до зловмисних замахів на інформаційні ресурси та потоки господарчого суб'єкта. Запропонована система захисту об'єктів інформації комп'ютерних мереж від незаконного відтоку інформації, а також охорони комерційної таємниці ґрунтується на законодавстві України, наукових розробках українських спеціалістів у сфері інформаційної безпеки та набутому підприємствами досвіді[3].

1.2 АНАЛІЗ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Нині загальна кількість нормативно-правових актів, що регламентують діяльність в сфері технічного захисту інформації в нашій державі, складає близько 150 одиниць.

Основу державного регулювання суспільних відносин в сфері ТЗІ становить Конституція України. До спеціального законодавства, що врегульовує дану галузь, належать Закони України: «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну систему конфіденційного зв'язку», «Про Концепцію Національної програми інформатизації», «Про науково - технічну інформацію» та інші.

Конституція України є основним джерелом права у галузі технічного захисту інформації.

❖ Відповідно до Конституції:

• забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу (стаття 17);

• кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції (стаття 31);

• ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України (стаття 32);

• кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань (стаття 34);

• кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності (стаття 41).

❖ Закон про інформацію:

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

❖ Закон про державну таємницю:

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних

носіїв та охороною державної таємниці з метою захисту національної безпеки України.

- ❖ Закон про захист інформації в інформаційно-телекомунікаційних системах:

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

- ❖ Закон про національну систему конфіденційного зв’язку:

Цей Закон регулює суспільні відносини, пов'язані із створенням, функціонуванням, розвитком та використанням Національної системи конфіденційного зв'язку.

- ❖ Закон про концепцію національної програми інформатизації:

Концепція Національної програми інформатизації включає арактеристику сучасного стану інформатизації, стратегічні цілі та основні принципи інформатизації, очікувані наслідки її реалізації

- ❖ Закон про науково - технічну інформацію:

Цей Закон визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни. Метою Закону є створення в Україні правової бази для одержання та використання науково-технічної інформації.

Законом регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі.

Дія Закону поширюється на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації. Дія Закону не поширюється на інформацію, що містить державну та іншу охоронювану законом таємницю.

Крім того, на сьогодні в Україні чинними є ряд нормативних документів (НД), що унормовують технічний захист інформації.

Це державні стандарти (ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення; ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт; ДСТУ 3396.2-96 Захист інформації. Технічний захист інформації. Терміни та визначення) та галузеві стандарти (НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу; НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу; НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу; НД ТЗІ 2.5- 005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу; НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі).

- ДСТУ 3396.2-96 Захист інформації. Технічний захист інформації. Терміни та визначення.

Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації (ТЗІ).Терміни, регламентовані у цьому стандарті, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації.

Терміни стандарту є обов'язковими для використання підприємствами та установами усіх форм власності і підпорядкування, громадянами - суб'єктами підприємницької діяльності, міністерствами (відомствами), центральними і місцевими органами державної виконавчої влади, військовими частинами усіх військових формувань, представництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить

державну чи іншу передбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

- ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення

Цей стандарт установлює об'єкт, мету, основні організаційнотехнічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.
Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян - суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

- ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації (ТЗІ).
Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів слід керуватися низкою нормативно-правових документів та актів. Базовими нормативними документами при організації та побудови комплексної системи захисту інформації в інформаційно-комунікаційних системах та мережах (далі ІКСМ) є:

- НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп’ютерних системах від НСД;
  Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:
  - визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;
  - створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
  - оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.
- НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;
  Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Терміни, що установлюються цим документом, обов’язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації
- НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі;
  Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - “Положення про службу захисту інформації в автоматизованій системі”.
- НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
  Цей стандарт установлює об’єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Основою для надійного та ефективного захисту являється вибір стандартного функціонального профілю захищеності згідно із НД ТЗІ 2.5-005-99 . Під поняттям функціонального профілю захищеності будемо розуміти перелік мінімально необхідних рівнів послуг та механізмів, які повинна реалізовувати система захисту ІКСМ. Функціональний профіль захищеності повинен задовольняти певні вимоги щодо захищеності інформації, яка обробляється в захищеній ІКСМ. Основними вимогами щодо захищеності інформації являється захист цілісності та доступності інформації та інформаційних ресурсів. Тому функціональний профіль захищеності для сучасних розгалужених ІКСМ приймає наступний вид: 3.ЦД.1-3.ЦД.4. Вибраний профіль захищеності дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх передачі через незахищене середовище та включає в себе обов’язкове проведення процедур ідентифікації і автентифікації.

Нормативно-правова база, яка регулює питання відносин між людьми в сфері захисту інформації постійно оновлюється та вдосконалюється. Оновлення документів засвідчує факт того, що із розвитком технологій, необхідно модернізувати юридичну базу. Враховуючи перелік документів формується розуміння того, що сфера захисту інформації являється достатньо великою та потребує більших сил для ведення правового

урегулювання, саме тому документи повинні оновлюватись частіше та цілісніше.

1.3 ПОСТАНОВКА ЗАДАЧІ

На період виконання дипломного проекту були сформовані та поставлені наступні задачі:

- виконання обстеження ОІД;
- аналіз ризиків;
- детальне обґрунтовування необхідності створення КСЗІ;
- розробка політики безпеки;
- розрахування трудоємності та затрат на створення та впровадження політики безпеки.

1.4 ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

В першому розділі було описано стан питання забезпечення інформаційної безпеки у інвестиційній діяльності, приведені основні проблеми із забезпеченням захисту інформації. Подано аналіз нормативно-правового забезпечення захисту інформації та поставлені задачі для подальшої роботи.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 ОБГРУНТУВАННЯ НЕОБХІДНОСТІ СТВОРЕННЯ КСЗІ

Згідно з 6 пунктом НД ТЗІ 3.7-003 -2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

6.1.1.1 Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.
6.1.1.2 Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

6.1.1.3 На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.
В ІІЦ циркулює інформація з обмеженим доступом (бази даних інвесторів, плани забудівель проектів) вимога щодо захисту якої встановлена законом,

повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

2.2 ЗАГАЛЬНІ ВІДОМОСТІ ПРО ПІДПРИЄМСТВО

Об’єктом дослідження являється Державне підприємство «Інформаційно-комунікаційний комплекс» (далі ІІЦ). Був започаткований в 2000р. під назвою «Адміністративно-господарське підприємство» В м. Дніпропетровську за адресою вул. Мостова, будинок 3. Але через недостатнє державне фінансування та непрофесійне керівництво, підприємство змінило власника та назву в 2008р. Зменшивши свій круг діяльності та сконцентрувавши сили на інвестиціях, грантах і проектах. У 2016 році ІІЦ взяло відповідальність за державний сайт igov, співпрацюючи з Облрадою Дніпровської області.

Завдяки діяльності підприємства в Україні буде збудований Індустріальний парк «Павлоград». Індустріальний парк «Павлоград» - це зона для прискореного розвитку промисловості та інновацій, парк з найбільшим потенціалом в Україні. Також в скарбниці підприємства є пошук інвесторів для відновлення ГЕС (наприклад, відновлення Шишацької ГЕС,Дулицької ГЕС). ІІЦ проводить щорічні конкурси «грантування», це виділення грошей переможцю і подальша допомога в реалізації проекту, тому не всі проекти підприємства пов’язані з державним сектором. Таким прикладом є ферма з вирощування та розведення бичків породи Абердин, задля подальшого виробництва мармурового м`яса. Або організація виробництва з переробки побутових відходів з виділенням з них пластику, придатного для вторинної переробки.

Отже, комплекс це окрема одиниця, що співпрацює з Облрадою Дніпровської області. За організаційно – правовою формою є Державним підприємством, але в інституційному секторі економіки є Державною нефінансовою корпорацією.

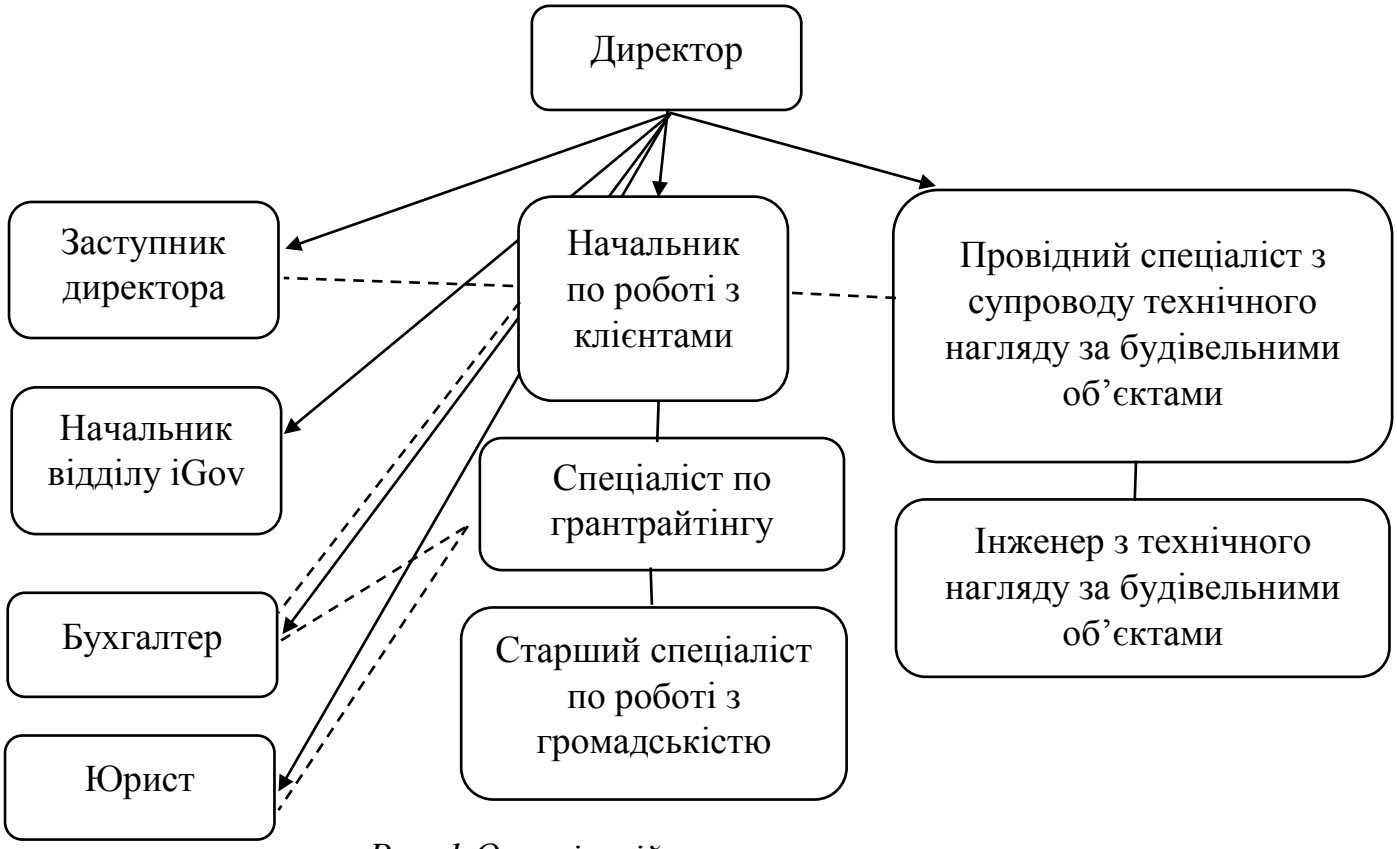

Рис. 1 Організаційна структура комплексу

Організаційна структура комплексу збудована за лінійно-функціональною ознакою. Штат комплексу становить 10 чоловік. Через це можна сказати, що усі працівники взаємодіють один з одним навіть якщо сфери їх діяльності не перетинаються. Комплекс знаходиться на території бізнес центру тому використовує охорону надану БЦ.

Комплекс функціонує згідно із чинним законодавством України.

1. Директор. Координує роботу усіх відділів. Дає інтерв'ю пресі та з'являється на телебаченні для популяризації комплексу. Обличчя ІІЦ.
2. Заступник директора. Допомагає координувати відділи. Слідкує за графіком, розробляє графік зустрічей директору. Редагує промови та виступи директора для медіа.

3. Бухгалтер. Веде бухгалтерію підприємства. Звітує перед Облрадою.
4. Юрист. Веде юридичну сторону діяльності комплексу. Головна позиція у грантрайтінгу, але за необхідності допомагає усім відділам комплексу.
5. Начальник відділу iGov. Відповідальний за роботу сайту iGov. Координує роботу розробників сайту, вносить інновації. Системний адміністратор центру за сумісництвом.
6. Начальник по роботі з клієнтами. Займається пошуком клієнтів, проектів та подальшим їх супроводом.
7. Спеціаліст по грантрайтінгу. Займається пошуком інвесторів для існуючих проектів.
8. Старший спеціаліст по роботі з громадськістю. Пише промови для директора. Веде усі соціальні медіа підприємства
9. Провідний спеціаліст з супроводу технічного нагляду за будівельними об’єктами. Координує діяльність будівельників. Погоджує та налагоджує плани будівельних робіт.
10. Інженер з технічного нагляду за будівельними об’єктами. Робить огляд та звітує за стан будівельних робіт і порядок їх проведення.

АНАЛІЗ ОБРОБЛЮВАНОЇ ІНФОРМАЦІЇ

Через ІІЦ кожного дня циркулює велика кількість інформації. Переважно це конфіденційна інформація така як листи від або до інвесторів, клієнтів, працівників інших фірм та інше. Також на працівники центру працюють з базами даних із конфіденційною інформацією.

Інформаційні потоки на підприємстві переважно в електронній формі, але також циркулює інформація на паперових носіях такі як заяви, звіти, акти. Усі працівники з’єднані між собою за допомогою Локальної мережі. В якій вони обмінюються виключно інформацією для загального доступу. Інформація приватна та конфіденційна поширюється через інтернет за

допомогою поштових сервісів таких як @gmail та @ukr.net. Усі листи від клієнтів резервно копіюються та зберігаються з моменту заснування фірми. Детальний перелік інформації, її правовий режим, вид зберігання та вимогу до захисту зображений в таблиці 1.

Схема зображення інформаційних потоків (далі ІП) наведена у рисунку 2.

К – вимоги до конфіденційності

Ц – вимога до цілісності

Д – вимога до доступності

Таблиця 1 «Оброблювана інформація»

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
1	База даних клієнтів	Електронний	ІЗоД	Комерційна таємниця	КЦД
2	Звіт господарчої діяльності	Електронний, паперовий	ІЗоД	Службова	КЦД
3	Фінансова звітність	Електронний, паперовий	ІЗоД	Службова	КЦД
4	База даних інвесторів	Електронний	ІЗоД	Службова	КЦД
5	Звіт про стан об’єктів будівництва	Електронний, паперовий	ІЗоД	Службова	КЦД
6	База даних партнерів	Електронний	Відкрита	-	Д
7	Формування та ведення реєстру форм звітних документів	Електронний	ІЗоД	Службова	КЦД
8	Внутрішня документація	Електронний	ІЗоД	Службова	КЦД
9	База даних	Електронний	ІЗоД	Службова	КЦД

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
	будівельних проектів				

Рис 2 Інформаційні потоки на підприємстві

2.2 ОБСТЕЖЕННЯ ОБ’ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Знаходиться за адресою Святослава Хороброго, 12. Підприємство розташувалось на 3 поверху Бізнес центру Цитадель. Центр підпорядкован Дніпропетровській обласній раді.

Інвестиційно-інноваційний центр є державним підприємством, що дає можливість налагодити ефективний діалог з органами місцевого самоврядування та прискорити процеси отримання супровідної документації для інвестиційних проектів на місцевому рівні.

Цитадель має 5 надземних поверхів, та 1 підземний, що є підземною парковкою. Приміщення комплексу знаходяться на третьому поверсі. Вікна приміщення виходять на житловий будинок навпроти, та на парковий майданчик для інкасаторських машин. За межі КЗ виходять кабелі електропостачання, труби опалення та каналізація.

Територія БЦ оздоблена зовнішнім контрольно-пропускним пунктом з турнікетом на центральному вході, а також зовнішніми кодовими дверима на півдні. На підприємстві встановлені камери за ініціативою директора фірми, що не підключені до чергового пункту, а передають інформацію тільки директору. На кожному поверсі будівлі розміщені камери відеоспостереження (на сходовому майданчику та в коридорі). Відеоспостереження ведеться з чергового пункту, який розташований на 1 поверсі. Центр працює пн-пт з 9:00 до 18.00, обідня перерва з 12:00 до 13:00.

Прибирання приміщення проводиться кожний четверг з 8 до 9 години ранку. Охорона цілодобова - надаються послуги приватної охорони. Охорона функціонує цілодобово та виконує регулярні нічні обходи. Зовнішні стіни будівлі виконані з бетону, фундамент будівлі – подушка з щебню. Дах виконаний з рубероїдної покрівлі.

Територія навколо будівлі з обстежуваним ОІД заасфальтована, навпроти головного входу трамвайна зупинка. Вхідні двері центрального входу

металопластикові, складаються з 3 блоків. Вхідні двері запасного входу металеві.

Оскільки будівля підприємства знаходиться майже у центрі міста, вона оточена іншими будівлями. Розташування БЦ показано в додатку А

Таблиця 3 – Прилеглі будівлі відносно ОІД

№	Тип споруди	Адреса	Кількість поверхів	Розташування відносно ОІД	Мінімальна відстань від ОІД до споруди
1	Торговий центр	вулиця Святослава Хороброго, 12А,	2	північ	15 метрів
2	Торговий центр	вулиця Січових Стрільців, 20,	5	схід	20 метрів
3	Житловий будинок	вулиця Січових Стрільців, 16,	5	Північ-схід	70 метрів
4	Житловий будинок	вул. Святослава Хороброго, 13	2	Північ-захід	30 метрів

Таблиця 4 – Прилеглі вулиці відносно ОІД

вул. Січових Стрільців	Знаходиться на сході відносно ОІД, в 10 метрах від ОІД, інтенсивність руху – 1000 автомобілів в годину, ширина проїжджої частини – 5 метрів (односмугова в північному напрямі), ширина пішохідної частини – 2 метри (2 метри ліворуч та 2 метри праворуч відносно

	вулиці), уздовж вулиці є можливість паркування.
вул. Святослава Хороброго	Знаходиться на півдні відносно ОІД, в 60 метрах від ОІД, ширина проїжджої частини – 8 метрів (односмугова в північному та південному напрямі), ширина пішохідної частини – 4 метри (2 метри ліворуч та 2 метри праворуч відносно вулиці), уздовж вулиці є можливість паркування.

Комунікаційні системи КЗ вказані у таблиці №5

Таблиця №5 «Комунікаційні системи»

Вид комунікацій	*Характеристика*
Система опалення	Підключена до міської мережі опалення «Теплоенерго», знаходиться за межами КЗ.
Електроживлення	Підключено до трансформаторної підстанції ТП № 43 «ДТЕК Дніпровські Електромережі», котра обслуговує сторонніх споживачів і виходить за межі КЗ.
Система водопостачання	Підключена до міського водоканалу «Водоканал», котрий виходить за межі КЗ
Система каналізації	Підключена до міської мережі каналізації, котра виходить за межі КЗ.
Система заземлення	Всі прилади, комп’ютери заземлені на спільний контур заземлення, котрий є замкненим і

Вид комунікацій	*Характеристика*
	виходить за межі КЗ.
Мобільний зв’язок	Мобільна лінія «Київстар». На всіх співробітників виділені мобільні номера. Виходить за межі КЗ. Є два стаціонарних телефона.
Лінія постачання мережі Інтернет	Підключена до Інтернет-провайдеру «Укртелеком», знаходиться за межами КЗ.

Таблиця 6 – Корпусний опис основних технічних засобів ДП ІІЦ

Тип	Ім’я	Інвентарний номер	Місце розташування	Мінімальна відстань до кордонів ОІД
Принтер	HP LaserJet 1018	20043929001	На столі	2100 мм
Маршрутизатор	TP-Link TL-WR841N	20043929010	На столі	200 мм
Системний блок	Lenovo IdeaCentre 300	20043929002	На підлозі	1300 мм
Системний блок	Lenovo IdeaCentre 300	20043929003	На підлозі	1300 мм
Системний блок	Lenovo IdeaCentre 300	20043929004	На підлозі	2000 мм
Системний блок	Lenovo IdeaCentre 300	20043929005	На підлозі	2000 мм
Монітор	LG 19EN33	200439290021	На столі	2000 мм
Монітор	LG 19EN33	200439290031	На столі	2000 мм
Тип	Ім’я	Інвентарний	Місце	Мінімальна

		номер	розташування	відстань до кордонів ОІД
Монітор	LG 19EN33	200439290041	На столі	1300 мм
Монітор	LG 19EN33	200439290051	На столі	1300 мм
Ноутбук	HP 15-g023er	20043929008	На столі	600 мм
Ноутбук	HP 15-g023er	20043929009	На столі	600 мм
Ноутбук	HP 15-g023er	20043929011	На столі	800 мм
Ноутбук	HP 15-g023er	20043929012	На столі	800 мм

Крім цього, на ОІД функціонують наступні ДТЗС

Таблиця 7– Опис елементів ДТЗС

Тип	Ім’я	Інвентарний номер	Місце розташування	Мінімальна відстань до кордонів ОІД
Мікрохвильова піч	Perfezza FZ-0719	20043929100	На столі	300 мм
Електрочайник	Vitek VT-7008	20043929101	На столі	300 мм
Електрочайник	Vitek VT-7008	20043929102	На столі	500 мм
Кондиціонер	LG CN-4921	20043929103	На стіні	350 мм
Дротовий телефон	Panasonic KX-TS2356	20043929104	На столі	100 мм
Дротовий телефон	Panasonic KX-TS2356	20043929105	На столі	300 мм
Датчик диму	Артон СПД-3	20043929106	На стелі	950 мм
Датчик диму	Артон СПД-3	20043929106	На стелі	1550 мм
Відеокамера	VStarcam C385	20043929107	На шафі	1000мм

Відеокамера	VStarcam C385	20043929108	На стіні	1000мм
ПКП	Тирас 4П	20043929109	На стіні	1300 мм

Характеристика обчислювальних систем вказані у таблиці №8

Характеристика КС ДП «ІІЦ»

Lenovo IdeaCentre 300: Core i3 2x2800 МГц, nVidia GTX 550 ti, 4096 МБ ОЗП, 256 ГБ SSD, материнська плата ASRock Socket 1155 Z77M, ОС Windows 10 Home Single – 5 шт.

Монітор LG 19EN33;

Ноутбук HP 15-g023er: Core i3-5005U, nVidia GeForce 920M і Intel HD 5500, 4096 МБ ОЗП, 512 ГБ SSD, ОС Windows 10 Home Single – 4 шт.

У зв’язку з тим, що є 2 види АРМ, розглянемо склад системи і склад ПЗ ноутбуків і комп’ютерів ОІД.

Таблиця 8 – Апаратний склад комп’ютера ДП «ІІЦ»

Тип	Повна назва	Серійний номер	Обсяг (Потужність)
Процесор	Core i3 2x2800 МГц	763Q6279-i3	–
Материнська плата	ASRock Socket 1155 Z77M	391MP53888/2	–
Графічний відеоадаптер	nVidia GTX 550 ti	392082SER/550ti	1024 Мб
ОЗП	Goodram DDR3 1300	RAM291073YT	4096 Мб
ПЗП (SSD)	Samsung Evo 860 SATA III	20374518195372-860	256 Гб
Монітор	LG 19EN33	LG920361192-EN33	–
Тип	Повна назва	Серійний номер	Обсяг (Потужність)

Блок живлення	V-Power 750QQ	2910Q92-750	750 Вт
Дротова клавіатура	Logitech K200	2073K949w71690	–
Дротова мишка	Logitech M100	302918M6371922T	–

Таблиця 9 – Апаратний склад ноутбука АС ДП «ІІЦ»

Тип	Повна назва	Серійний номер	Обсяг (Потужність)
Процесор	Core i3 2x2800 МГц	763Q6279-i3	–
Материнська плата	Globex MPlate P3310	U6382I03729	–
Графічний відеоадаптер	nVidia GeForce 920M	209641SER/920M	2048 Мб
Інтегрований відеоадаптер	Intel HD 5500	8930201T94302-5500	2048 Мб
ОЗП	HyperX 3D 2133	203846820O	4096 Мб
ПЗП (SSD)	Grotex Speed+ L2 SATA 2.5	8392916JJ829ON	512 Гб
Дротова мишка	Logitech M310	1825LZ002379	–

Таблиця 10 – Склад ПЗ комп'ютера АС ДП «ІІЦ»

№	Повна назва	Тип ПЗ	Версія ПЗ	Наявність ліцензії	Кількість ПЗ
А	nVidia GeForce Experience	Системне	3.17.0.126	Є	4
Б	DriverPack Solution	Системне	17.7.56	Немає	4
В	Win7_8_10x64_LG 19EN33_driver	Драйвери	12.92.007	Є	4
Г	Google Chrome	Прикладне	72.0.3626.105	Є	4
Ґ	Opera	Прикладне	58.0.3135.47	Є	4
Д	FileZilla	Прикладне	3.40.0	Є	2
Е	Skype	Прикладне	8.38.0.138	Є	4
Є	Viber	Прикладне	10.2.0.38	Є	4
Ж	Telegram Desktop	Прикладне	5.4.0	Є	4
З	Microsoft Office 2013 SP1 Standart	Прикладне	15.0.4833.1000	Немає	4
И	ESET NOD 32	Спеціалізоване	12.0.27.0	Немає	4
І	Notepad++	Прикладне	62.0	Є	3
Й	TesauRUS	Прикладне	5.4.12	Немає	1
К	Windows 10 Home Single	Системне	10.01776	Є	4

Таблиця 11 – Склад ПЗ ноутбука ДП «ІІЦ»

№	Повна назва	Тип ПЗ	Версія ПЗ	Наявність ліцензії	Кількість ПЗ
	nVidia GeForce Experience	Системне	3.17.0.126	Є	4
	DriverPack Solution	Системне	17.7.56	Немає	4

№	Повна назва	Тип ПЗ	Версія ПЗ	Наявність ліцензії	Кількість ПЗ
Л	HP_LJ1018_driver_win 10x64_win7x64	Драйвери	3.02.198	Є	1
	Google Chrome	Прикладне	72.0.3626.105	Є	4
	Opera	Прикладне	58.0.3135.47	Є	4
М	TeamViewer	Прикладне	3.40.0	Є	1
	Skype	Прикладне	8.38.0.138	Є	4
	Viber	Прикладне	10.2.0.38	Є	4
	Telegram Desktop	Прикладне	5.4.0	Є	4
	TesauRUS	Прикладне	5.4.12	Немає	2
	Microsoft Office 2013 SP1 Standart	Прикладне	15.0.4833.1000	Немає	4
	ESET NOD 32	Спеціалізоване	12.0.27.0	Немає	4
	Notepad++	Прикладне	62.0	Є	2
	Windows 10 Home Single	Системне	10.01776	Є	4

На підприємстві використовується АС класу 3 - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Де є необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Локальна мережа фізично має архітектуру «зірка». Вихід в інтернет здійснюється через кабель Ethernet підключеного до Wi-Fi роутера, з'єднання здійснюються за допомогою екранованого кабелю «вита пара».

Обладнання, за допомогою якого оброблюється інформація на ОІД:

1. Комп’ютер директора підприємства

2. Комп’ютер бухгалтера

3. Комп’ютер юриста

4. Комп’ютер керівника відділу Igov

6. Ноутбук старшого спеціаліста по роботі з громадськістю

8. Комп’ютер начальника по роботі з клієнтами

9. Ноутбук спеціалісту по грантрайтінгу.

10. Ноутбук заступника директора

Комп’ютери штатних працівників належать до єдиної робочої групи «WORK». Співробітникам охоронної компанії, які займаються моніторингом камер відеоспостереження доступ до робочої групи не надається. Функціональна схема мережі наведена малюнку №3.

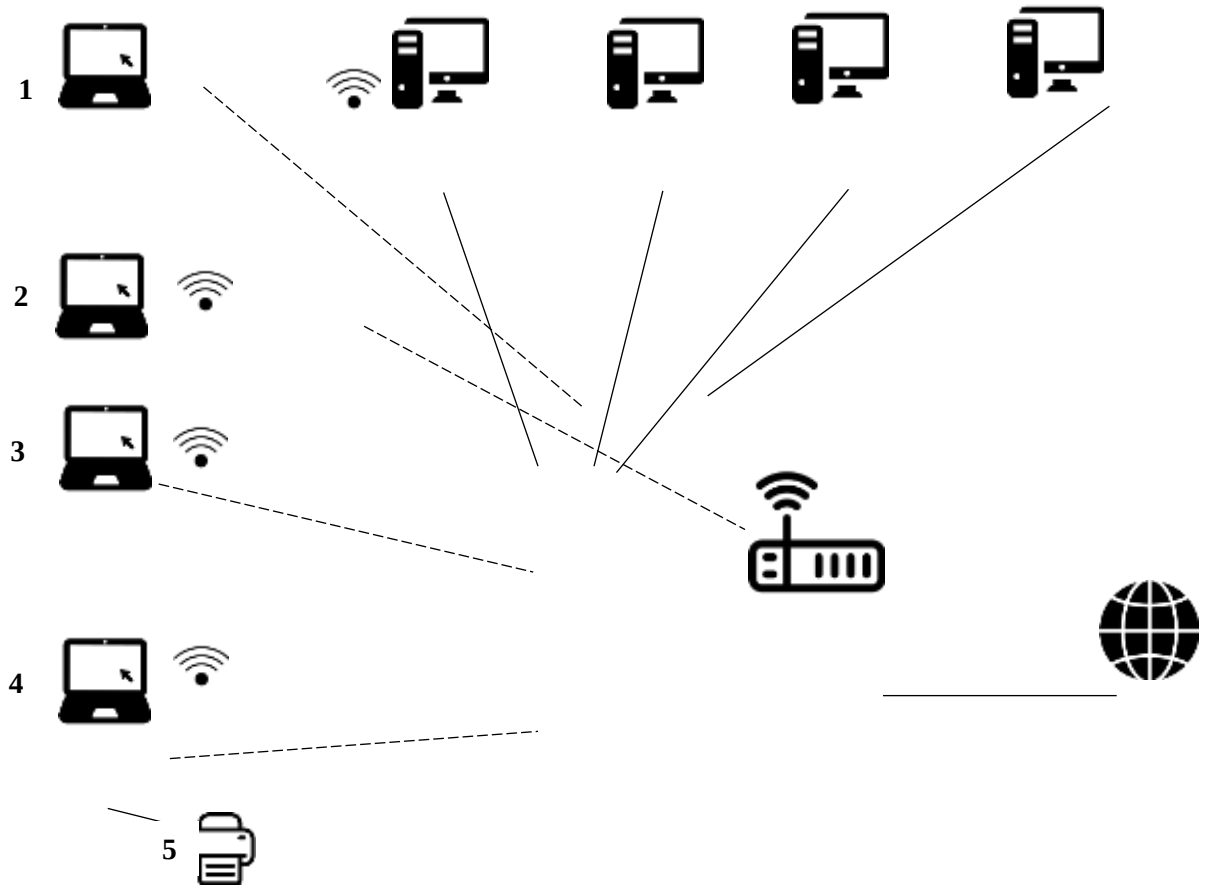

Рис 3 Функціональна схема мережі ДП «ІІЦ»

2.3 АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ

Для побудови політики безпеки та комплексних систем захисту, в першу чергу необхідно провести аналіз загроз та вразливостей інформаційної безпеки підприємства.

Джерела загроз інформаційній безпеці поділяються на три основні групи:

- Антропогенні (обумовлені діями суб'єкта)
- Техногенні (обумовлені технічними засобами)
- Стихійні

Загрози визначаються коефіцієнтом рівня небезпеки $К_{неб}$ наступною формулою:

$$К_{неб} = \frac{К1 \times К2 \times К3}{125}$$

125- це максимальне число добутку показників $К_{неб}$

Розглянемо перелік антропогенних джерел загроз та вразливостей:

Для антропогенних джерел:

К1 – ступінь доступності до об'єкту;

К2 – ступінь кваліфікації і мотивації;

К3 – рівень наслідків (фатальність).

Таблиця 10 Перелік можливих антропогенних джерел загроз

№	Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
1	Директор	5	2	5	50	0,400
2	Заступник директора	5	3	5	75	0,600
3	Бухгалтер	4	2	4	32	0,256
4	Юрист	3	2	3	18	0,144
5	Керівник відділу Igov	4	4	4	64	0,512

№	Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
6	Старший спеціаліст по роботі з громадськістю	3	3	3	27	0,216
7	Начальник по роботі з клієнтами	4	2	4	32	0,256
8	Спеціаліст з грантрайтінгу	3	2	4	24	0,192
9	Допоміжний персонал (прибиральниця)	1	3	1	3	0,024
10	Хакери	1	4	4	16	0,128
11	Конкуренти	1	3	5	15	0,120

Для класифікації вразливостей визначаються наступні критерії:

К1 – ступінь впливу вразливості на неусунення наслідків (фатальність);

К2 – можливість (зручність) використання вразливості джерелом загроз

К3 – кількість елементів об’єкту.

Таблиця 11 Об’єктивні вразливості

Вразливість	К1	К2	К3	К1*К2*К3	$К_{неб}$
1. Вразливості, що активізуються					
1.1 Апаратні закладки	3	3	3	27	0.216
1.2 Неліцензоване ПЗ	3	4	2	24	0.192
2. Вразливості, які обумовлені особливостями елементів					
2.1 Елементи з електроакустичним перетворенням	4	3	5	60	0.480
3. Вразливості, які обумовлені особливостями захищеного об’єкту					
3.1 Місцезнаходження об’єкту	3	3	3	27	0.216
3.2 Стихійні лиха	5	1	1	5	0.040

3.3 Перебої електропостачання	3	3	3	27	0.216

Таблиця 12 Суб'єктивні вразливості

Вразливість	К1	К2	К3	К1*К2*К3	$К_{неб}$
1. Помилки					
4.1 Помилки користувачів системи	3	3	2	27	0.216
4.2 Помилки при підготовці та використанні програмного забезпечення	3	3	2	18	0.144
4.3 Помилки при експлуатації технічних засобів обміну інформацією	4	3	3	36	0.288
2. Порушення					
5.1 Порушення режиму використання інформації	3	5	3	45	0.360
5.2 Порушення режиму конфіденційності	4	5	5	100	0.800

Таблиця 13 Взаємозв'язок джерел загроз і об'єктивних вразливостей

Джерело загроз	$К_{неб}$ (д.з.)	Вразливість	$К_{неб}$ (вр.)	$К_{неб}$
Директор	0.400	1.1 Апаратні закладки	0.216	0.008
		1.2 Неліцензоване ПЗ	0.192	0.007
		2.1 Елементи з електроакустичним перетворенням	0.480	0.019
		3.1 Місцезнаходження об'єкту	0.216	0.008
Заступник генерального	0.370	1.1 Апаратні закладки	0.216	0.008

директора		1.2 Неліцензоване ПЗ	0.192	0.007
		2.1 Елементи з електроакустичним перетворенням	0.480	0.019
		3.1 Місцезнаходження об’єкту	0.216	0.008
Юрист	0.364	1.1 Апаратні закладки	0.216	0.013
		1.2 Неліцензоване ПЗ	0.192	0.012
		2.1 Елементи з електроакустичним перетворенням	0.480	0.030
		3.1 Місцезнаходження об’єкту	0.216	0.013
Керівник відділу Igov	0.742	1.1 Апаратні закладки	0.216	0.172
		1.2 Неліцензоване ПЗ	0.192	0.153
		2.1 Елементи з електроакустичним перетворенням	0.480	0.384
		3.1 Місцезнаходження об’єкту	0.216	0.172
Старший спеціаліст по роботі з громадськістю	0.156	1.1 Апаратні закладки	0.216	0.012
		1.2 Неліцензоване ПЗ	0.192	0.010
		2.1 Елементи з електроакустичним перетворенням	0.480	0.026
		2.2Місцезнаходження об’єкту	0.216	0.012
Джерело загроз	$К_{неб}$ (д.з.)	Вразливість	$К_{неб}$ (вр.)	$К_{неб}$

Бухгалтер	0.023	1.1 Апаратні закладки	0.216	0.012
		1.2 Неліцензоване ПЗ	0.192	0.010
		a. Місцезнаходження об’єкту	0.216	0.012
Начальник по роботі з клієнтами	0.056	1.1 Апаратні закладки	0.216	0.012
		1.2 Неліцензоване ПЗ	0.192	0.010
		2.1 Елементи з електроакустичним перетворенням	0.480	0.026
		3.1 Місцезнаходження об’єкту	0.216	0.012
Спеціалісту по грантрайтінгу	0,156	1.1 Апаратні закладки	0.216	0.055
		1.2 Неліцензоване ПЗ	0.192	0.049
		2.1 Елементи з електроакустичним перетворенням	0.480	0.122
		3.1 Місцезнаходження об’єкту	0.216	0.055
Хакери	0.470	1.1 Апаратні закладки	0.216	0.086
		1.2 Неліцензоване ПЗ	0.192	0.076
		2.1 Елементи з електроакустичним перетворенням	0.480	0.192
		3.1 Місцезнаходження об’єкту	0.216	0.086

Джерело загроз	$К_{неб}$ (д.з.)	Вразливість	$К_{неб}$ (вр.)	$К_{неб}$
Конкуренти	0,400	1.1 Апаратні закладки	0.216	0.086
		2.1 Елементи з електроакустичним перетворенням	0.480	0.276

Таблиця 14 Взаємозв'язок джерел загроз і суб'єктивних вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Директор	0.400	4.1 Помилки користувачів системи	0.216	0.008
		4.2 Помилки при підготовці та використанні програмного забезпечення	0.144	0.005
		4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.188	0.011
		5.1 Порушення режиму використання інформації	0.360	0.014
		5.2 Порушення режиму конфіденційності	0.800	0.032
Заступник директора	0.400	4.1 Помилки користувачів системи	0.216	0.008
		4.2 Помилки при підготовці та використанні програмного забезпечення	0.144	0.005
		4.3 Помилки при експлуатації технічних	0.288	0.011

		засобів обміну інформацією		
		5.1 Порушення режиму використання інформації	0.360	0.014
		5.2 Порушення режиму конфіденційності	0.800	0.032
Юрист	0.464	4.1 Помилки користувачів системи	0.216	0.013
		4.2 Помилки при підготовці та використанні програмного забезпечення	0.144	0.009
		4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288	0.018
		5.1 Порушення режиму використання інформації	0.360	0.023
		5.2 Порушення режиму конфіденційності	0.800	0.051
Керівник відділу Igov	0.740	4.1 Помилки користувачів системи	0.216	0.172
		4.2 Помилки при підготовці та використанні програмного забезпечення	0.144	0.115
		4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288	0.230
		5.1 Порушення режиму використання інформації	0.360	0.288
		5.2 Порушення режиму конфіденційності	0.800	0.640

Бухгалтер	0.156	4.1 Помилки користувачів системи	0.216	0.012
		4.2 Помилки при підготовці та використанні програмного забезпечення	0.144	0.007
		4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288	0.016
		5.1 Порушення режиму використання інформації	0.360	0.020
		5.2 Порушення режиму конфіденційності	0.800	0.044
Начальник по роботі з клієнтами	0.156	4.1 Помилки користувачів системи	0.216	0.012
		4.2 Помилки при підготовці та використанні програмного забезпечення	0.144	0.007
		4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288	0.016
		5.1 Порушення режиму використання інформації	0.360	0.020
		5.2 Порушення режиму конфіденційності	0.800	0.044
Спеціалісту по грантрайтінгу	0.256	4.1 Помилки користувачів системи	0.216	0.055
		4.2 Помилки при підготовці та використанні	0.144	0.036

		програмного забезпечення		
		4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288	0.073
		5.1 Порушення режиму використання інформації	0.360	0.092
		5.2 Порушення режиму конфіденційності	0.800	0.204
Хакери	0.520	4.1 Помилки користувачів системи	0.216	0.086
		4.2 Помилки при підготовці та використанні програмного забезпечення	0.144	0.057
		4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288	0.115
		5.1 Порушення режиму використання інформації	0.360	0.144
		5.2 Порушення режиму конфіденційності	0.800	0.32

Загрози, з коефіцієнтом **нижче 0,2** вважаються неактуальними.

Використовуючи дані з таблиць 10 - 14 проведемо аналіз найбільш небезпечних загроз.

Таблиця 15 Аналіз найнебезпечніших загроз

Джерело загроз	Загроза	$К_{неб}$
Антропогенні суб’єктивні		
Директор	5.1 Порушення режиму використання інформації	0.360
	5.2 Порушення режиму конфіденційності	0.800
	4.1 Помилки користувачів системи	0,216
Заступник директора	4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288
	5.1 Порушення режиму використання інформації	0.360
	5.2 Порушення режиму конфіденційності	0.800
Юрист	4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288
	5.1 Порушення режиму використання інформації	0.360
	5.2 Порушення режиму конфіденційності	0.800
Керівник відділу Igov	4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288
	5.1 Порушення режиму використання інформації	0.360
	5.2 Порушення режиму	0.800

	конфіденційності	
Бухгалтер	4.1 Помилки користувачів системи	0.216
	5.1 Порушення режиму використання інформації	0,110
	5.2 Порушення режиму конфіденційності	0,800
Начальник по роботі з клієнтами	4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288
	5.1 Порушення режиму використання інформації	0.360
	5.2 Порушення режиму конфіденційності	0.800
Спеціалісту по грантрайтінгу	4.3 Помилки при експлуатації технічних засобів обміну інформацією	0.288
	5.1 Порушення режиму використання інформації	0.360
	5.2 Порушення режиму конфіденційності	0.800
Антропогенні об’єктивні загрози		
Директор	2.1 Елементи з електроакустичним перетворенням	0.480
Керівник відділу Igov	5.2 Порушення режиму конфіденційності	0.800

2.4 Модель порушника

Якщо існує інформаційна система, у якій циркулює інформація з обмеженим доступом та конфіденційні дані, то знайдеться особа (порушник), метою якої буде ознайомлення з інформацією, її модифікація чи знищення. Для того, щоб розробити комплекс заходів по забезпеченню захищеності інформаційних ресурсів, необхідно побудувати модель можливого порушника. Ця модель може бути побудована з урахування різних критеріїв.

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх.[5]

Таблиця 16 Ймовірні внутрішні порушники

№	Джерело загроз	Коефіцієнт небезпеки
Антропогенні суб’єктивні		
1	Директор	0,400
2	Заступник директора	0,400
3	Бухгалтер	0,156
4	Юрист	0,464
5	Керівник відділу Igov	0,746
6	Старший спеціаліст по роботі з громадськістю	0,400
7	Начальник по роботі з клієнтами	0,156
8	Спеціаліст з грантрайтінгу	0,256
9	Допоміжний персонал (прибиральниця)	0,024
Антропогенні об’єктивні		

1	Директор	0,400
2	Заступник директора	0,370
3	Бухгалтер	0,024
4	Юрист	0,364
5	Керівник відділу Igov	0,742
6	Старший спеціаліст по роботі з громадськістю	0,156
7	Начальник по роботі з клієнтами	0,056
8	Спеціаліст з грантрайтінгу	0,156
9	Допоміжний персонал (прибиральниця)	0,024
Техногенні		
1	Елементи з електроакустичним перетворенням	0,480
2	Апаратні закладки	0.216
3	Неліцензоване ПЗ	0.192
4	Елементи з електроакустичним перетворенням	0.480
5	Місцезнаходження об’єкту	0.216

Таблиця 17 Ймовірні зовнішні порушники

№	Джерело загроз	Коефіцієнт небезпеки
1	Конкуренти	0,320
2	Хакери	0,370

Найбільшу небезпеку для підприємства становить Керівник відділу IGov, оскільки має найбільші коефіцієнти із суб'єктивних 0,746 і об'єктивних джерел 0,742. Із техногенних джерел найнебезпечнішими елементи з електроакустичним перетворенням та порушення статуту конфіденційності з коефіцієнтами 0,480 і 0,800 відповідно.

2.5 Розробка політики безпеки

1. Мета політики безпеки

Політика безпеки – це набір правил, вимог, рекомендацій до проведення інформаційної діяльності на підприємстві. Правильно виконана політика безпеки є запорукою інформаційної захищеності. Головною метою розробки політики є мінімізація ризиків для ведення бізнесу, забезпечення безперервності його функціонування. Це досягається за допомогою певних вимог до персоналу та інформації.

2. Область дії

Областю дії даної політики безпеки є державне підприємство Інформаційно-комунікаційний комплекс.

3. Відповідальний за виконання політики безпеки

Відповідальною особою за виконання інструкції є керівник IGov.

4. Інструкція

- Будь-яка інформація з обмеженим доступом повинна оброблятися на комп'ютерах, ноутбуках, що належать підприємству.

- На усіх комп’ютерах підприємства не повинно бути неліцензованого ПО.
- Не зважаючи на степінь довіри до працівника, кожен працівник повинен мати власний обліковий запис. Що був виданий системним адміністратором за розпорядженням заступника директора або директора.
- Кожен комп’ютер повинен бути захищений антивірусом.

5 Затвердження політики

Політика безпеки розробляється системним адміністратором та підписується директором підприємства / начальником відділу при прийнятті усіх розділів політики.

6 Дії з виконання інструкції інформаційної безпеки

Системний адміністратор контролює підключення до мережі, та має засоби моніторингу та виконання політики доступу.

7 Відповідальність

Керівник IGov несе відповідальність за виконання інструкції.

Оскільки на підприємстві циркулює не тільки електрона інформація, а працівники іноді залишають важливі документи на робочому місці, політика чистого столу буде доречна для ІІЦ.

Політика чистого столу

1. Короткий огляд

Політика чистого столу може бути важливим інструментом, що гарантує, що всі секретні\конфіденційні матеріали видалено з робочого простору кінцевого користувача та матеріали знаходяться під замком коли вони не використовуються або коли робітник знаходиться не на своєму робочому місці. Це одна з найкращих стратегій для впровадження, щоб зменшити ризик порушення безпеки на робочому місці. Така політика також може підвищити поінформованість працівника про захист секретної інформації.

2. Мета

Мета цієї політики є встановлення мінімальних вимог до підтримки «Чистого столу» - де інформація про наших робітників, інтелектуальної власності, покупців, постачальників знаходиться у безпеці в закритих місцях та поза зоною загального доступу. Політика Чистого столу це не тільки ISO 27001/17799, вона також є частиною базового стандарту контролю приватності.

3. Сфера застосування

Політика застосовується до всіх робітників та дочірніх відділень ІІЦ.

4. Політика

4.1 Робітники зобов'язані гарантувати, що уся секретна\конфіденційна інформація у друкованому або електронному вигляді захищена на їх робочому місці наприкінці дня та коли вони залишають робоче місце на довгий термін.

4.2 Комп'ютер повинен бути заблокований коли робоче місце вільне.

4.3 Комп'ютер повинен бути вимкнений після завершення робочого дня.

4.4 Будь-яка Службова\Обмежена або Секретна інформація повинна бути видалена зі столу та замкнена у шухляду коли стіл вільний або наприкінці робочого дня.

4.5 Шухляди для файлів, що містять інформацію для службового використання або конфіденційну повинні бути зачинені коли інформація не використовується.

4.6 Ключі, за допомогою яких можна отримати доступ до інформації для службового використання або конфіденційної інформації не повинні залишатися без нагляду.

4.7 Ноутбук повинен бути зафіксований спеціальним кабелем або схований у шухляду, що можна замкнути ключем.

4.8 Пароль не повинен бути написаний на липкому нотатку та залишений на або під комп’ютером. Він не повинен бути записаним у легкодоступних місцях.

4.9 Папери, що містять інформацію для службового використання або конфіденційну інформацію одразу повинні бути забрані.

4.10 Документи з інформацію для службового використання або з конфіденційною інформацією слід знищувати за допомогою шредера або викидати у зачинені приватні ящики для сміття.

4.11 Якщо службова\обмежена інформація була написана на дошці, після використання інформація повинна бути стерта.

4.12 Портативні пристрої повинні знаходитися у зачиняємій шухляді.

4.13 Необхідно відноситися до носіїв даних таких як CDROM, DVD або USB, як до носіїв обмеженої інформації. Та після використання тримати їх у зачиняємій шухляді.[6]

межах ІІЦ

Політика етики

1. Короткий огляд

ІІЦ зобов'язується захищати працівників, партнерів, постачальників та саму компанію від неправомірних або дій, що можуть завдати шкоди, окремих осіб, завданих свідомо чи несвідомо. Коли проблеми ІІЦ активно вирішуються та використовують правильне судження, це допоможе компанії випередити конкурентів.

ІІЦ не буде терпіти будь-яких правопорушень або невідповідностей в будь-який час. ІІЦ вживатиме відповідні заходи, щоб швидко виправити проблему, якщо етичність порушена.

2. Мета

Мета цієї політики створити культуру відкритості, довіри та наголосити на очікуваннях працівника та споживача, що до них будуть ставитись відповідно до справедливої ділової практики. Ця політика буде служити для

ведення бізнес-вихованості, щоб забезпечити етичну поведінку. Ефективна етика - це командні зусилля, що передбачають участь та підтримку кожного співробітника ІІЦ. Всі працівники повинні ознайомитися з керівними принципами етики, які слідують за цим вступом.

3. Сфера застосування

Ця політика стосується усіх робітників, підрядників, консультантів, тимчасових працівників та інших працівників в компанії ІІЦ, включаючи увесь персонал, що пов'язаний з третіми сторонами.

4. Політика

4.1 Зобов'язання з етики для керівників

4.1.1 Найважливішим прикладом мають стати провідні керівники та керівники компанії в межах ІІЦ. У будь-якій діловій практиці чесність та стійкі моральні принципи повинні бути головним пріоритетом для керівників.

4.1.2 Керівники повинні проводити політику відкритих дверей і вітати пропозиції та зауваження співробітників. Це дозволить працівникам почувати себе комфортно, обговорюючи будь-які проблеми, і попередить керівників про проблеми серед робітників.

4.1.3 Керівники повинні розкривати будь-який конфлікт інтересів, що має відношення до їх становища в межах ІІЦ

4.2 Зобов’язання з етики для робітників.

4.2.1 ІІЦ співробітники будуть ставитися до всіх чесно, мати взаємну повагу, сприяти робочому середовищу та уникати намірів і появи неетичних або компрометуючих практик.

4.2.2 Кожен співробітник повинен застосовувати зусилля та інтелект додержуючись етичних цінностей.

4.2.3 Працівники повинні розкривати будь-який конфлікт інтересів, що має відношення до їх становища в межах ІІЦ

4.2.4 Працівники будуть допомагати ІІЦ підвищити рівень задоволеності клієнтів та постачальників шляхом надання якісних продуктів та своєчасної відповіді на запити.

4.2.5 Співробітники повинні самостійно задати наступні питання, якщо поведінка є сумнівною:

• Чи поведінка є законною?

• Чи відповідає поведінка всім відповідним правилам ІІЦ?

• Чи відображає поведінка цінності та культуру ІІЦ?

• Чи може поведінка негативно вплинути на зацікавлених сторін компанії?

• Чи почуватиметесь ви занепокоєно, якщо така поведінка з'явиться у газетах?

• Чи може поведінка негативно впливати на ІІЦ, якщо всі співробітники це зробили?

4.3 Обізнаність компанії

4.3.1. Заохочення етичної поведінки в межах міжособистісних комунікацій працівників буде нагороджено.

4.3.2 ІІЦ буде сприяти створенню надійної та чесної атмосфери для посилення бачення етики всередині компанії.

4.4 Збереження етичних норм

4.4.1 ІІЦ посилить важливість повідомлення про цілісність, і почне зверху. Кожен співробітник, менеджер, директор повинен постійно підтримувати етичну позицію і підтримувати етичну поведінку.

4.4.2 Співробітники компанії ІІЦ повинні заохочувати відкритий діалог, отримувати чесний зворотний зв'язок і ставитися до всіх чесно і об'єктивно.

4.4.3 ІІЦ заснував комітет з розкриття кращої практики, щоб переконатися, що етичні правила доставляються всім співробітникам і що проблеми, пов'язані з правилами, можуть бути усунені.

4.4.4. Співробітники зобов'язані повторно стверджувати свою відповідність етичній політиці на щорічній основі.

4.5 Неетична поведінка

4.5.1 ІІЦ дозволить уникнути намірів і проявів неетичної або компрометуючої практики у відносинах, діях і зв'язках.
4.5.2 ІІЦ не терпітиме переслідування або дискримінацію.
4.5.3 Не допускається несанкціоноване використання комерційної таємниці, маркетингу, операційної, кадрової, фінансової, вихідної документації та технічної інформації, що є невід'ємною частиною успіху нашої компанії.
4.5.4 ІІЦ не допускатиме порушення в будь-який час, і ми будемо діяти етично і відповідно до законів.
4.5.5 ІІЦ Співробітники не будуть використовувати корпоративні активи або ділові відносини для особистого використання або отримання прибутку.[7]

Політика бездротового зв'язку

1. Огляд

З масовим вибухом смартфонів і планшетів, поява бездротового зв'язку, як альтернативи для кабельного інтернету вже давно є розповсюдженим на підприємствах. Небезпечна бездротова конфігурація може забезпечити легкі відкриті двері для зловмисників.

2. Мета

Метою цієї політики є забезпечення та захист інформаційних активів, що належать компанії ІІЦ. ІІЦ використовує комп'ютерні пристрої, мережі та інші електронні інформаційні системи для виконання завдань, цілей та ініціатив. ІІЦ надає доступ до цих ресурсів як привілей і повинна керувати ними відповідально для збереження конфіденційності, цілісності та доступності всіх інформаційних активів.

Ця політика визначає умови, яким повинні відповідати пристрої бездротової інфраструктури для підключення до мережі ІІЦ. Лише ті пристрої інфраструктури бездротового зв'язку, які відповідають стандартам,

визначеним у цій політиці, або надані Департаментом інформаційної безпеки виключення, схвалені для підключення до мережі ІІЦ.

3. Обсяг

Усі працівники, підрядники, консультанти, тимчасові та інші працівники на ІІЦ, включаючи всіх співробітників, пов'язаних з третіми особами, які підтримують пристрій бездротової інфраструктури від імені ІІЦ, повинні дотримуватися цієї політики. Ця політика застосовується до всіх бездротових інфраструктурних пристроїв, які підключаються до мережі ІІЦ або знаходяться на сайті ІІЦ, який забезпечує бездротове підключення до кінцевих пристроїв, включаючи ноутбуки, настільні комп'ютери, стільникові телефони та планшети. Це включає будь-яку форму пристрою бездротового зв'язку, здатного передавати пакетні дані.

4. Політика

4.1 Загальні вимоги

Всі пристрої інфраструктури бездротового зв'язку, які знаходяться на сайті ІІЦ і підключаються до мережі ІІЦ або надають доступ до інформації, що класифікується як ІІЦ Конфіденційно, або вище, повинні:

• Дотримуватися стандартів, зазначених у стандарті бездротового зв'язку.

• Бути встановленою, підтримуваною та підтримуваною затвердженою групою підтримки.

• Використовуйте у ІІЦ затверджені протоколи аутентифікації та інфраструктуру.

• Використовуйте протоколи шифрування в ІІЦ.

• Підтримувати апаратну адресу (MAC-адресу), яка може бути зареєстрована та відстежена.

• Не заважати розгортанню бездротового доступу, що підтримується іншими організаціями підтримки.

4.2 Вимоги до лабораторних та ізольованих бездротових пристроїв

Всі пристрої інфраструктури бездротової мережі, які надають доступ до ІІЦ Конфіденційно або вище, повинні відповідати розділу 4.1 вище. Лабораторні та ізольовані бездротові пристрої, які не надають загальну мережу підключення до мережі ІІЦ, повинні:

• Будьте ізольованими від корпоративної мережі (тобто не повинні надавати жодних корпоративних можливостей підключення) і виконувати політику безпеки лабораторії.

• Не заважати розгортанню бездротового доступу, що підтримується іншими організаціями підтримки.

Побудуємо таблицю для аналізу зменшення ризику після введення політик безпеки на підприємстві

Загрози	До введення політик	Після введення політик
Об’єктивні вразливості		
1.1 Апаратні закладки	0.192	0,100
1.2 Неліцензоване ПЗ	0.216	0.016
2.1 Елементи з електроакустичним	0.480	0,150

перетворенням		
4. Вразливості, які обумовлені особливостями захищеного об’єкту	0,480	0,400
3.1Місцезнаходження об’єкту	0,216	0,216
3.2 Стихійні лиха	0,040	0,040
3.3 Перебої електропостачання	0,216	0,216
Суб’єктивні вразливості		
4.1 Помилки користувачів системи	0,216	0,216
4.2 Помилки при підготовці та використанні програмного забезпечення	0,144	0,010
4.3 Помилки при експлуатації технічних засобів обміну інформацією	0,288	0,288
5.1 Порушення режиму використання інформації	0,360	0,100
5.2 Порушення режиму конфіденційності	0,800	0,300

Загрози, що мали істотне значення для безпеки підприємства після введення політик безпеки мають значно нижчу міру ризику.

Висновки до другого розділу

Під час виконання другого розділу, було виконано обґрунтування створення необхідності комплексної системи захисту інформації, встановлено, яка інформація циркулює у ІІЦ. Були розглянуті загальні

відомості про підприємство, проведено обстеження об’єкту інформаційної діяльності, зроблена класифікація інформації, зроблений аналіз інформаційних потоків, що циркулюють на підприємстві, виконаний аналіз загроз та вразливостей системи, розроблена модель порушника, проведений аналіз ризиків для виявлення слабких місць у системі забезпечення інформаційної безпеки.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Розрахунок вартості політики безпеки

Метою виконання економічного розділу дипломного проекту є техніко-економічне обґрунтування доцільності запровадження запропонованих в проекті рішень відповідно до обраної теми. Основною задачею техніко-економічного обґрунтування є визначення економічної ефективності використання основних та супутніх результатів, що мають бути отримані при виконанні дипломного проекту.

1. *Визначення трудомісткості розробки політики безпеки інформації*

$t = t_{тз} + t_{в} + t_{а} + t_{взз} + t_{озб} + t_{овр} + t_{д}$, годин,

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{взз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

2. Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації ***Крп*** складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки ***Ззп*** і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації ***Змч***:

$$К_{рп} = З_{зп} + З_{мч}$$

$$З_{зп} = t \cdot З_{іб}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t \cdot С_{мч}$$

де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot Се + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}}, \text{ грн,} \qquad (2.5)$$

де P – встановлена потужність ПК, кВт;

$С_{е}$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_{а}$ – річна норма амортизації на ПК, частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}\ , \qquad (2.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{рп}$ – вартість розробки політики безпеки інформації, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

Розрахунок поточних (експлуатаційних) витрат

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}\ ,\quad \text{тис. грн}$$

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$Ск= С_н + С_а + С_з + С_{єв}+ С_е + С_{ел} + С_о + С_{тос}, \text{ грн}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо ($С_н$).

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) (табл. Додатка).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} \text{ , грн.}$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн,} \qquad (2.11)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин.

Витрати на залучення сторонніх *організацій* для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) визначаються за даними організації.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%).

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, користуючись даними табл. 1 про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

3.1. Оцінка величини збитку

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- ❖ порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- ❖ порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- ❖ порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- ❖ порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \ , \qquad (3.2)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.3)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{Ви} = \frac{\sum Зс}{F} \cdot t_{ви} \ . \qquad (3.4)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \ . \qquad (3.5)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{Fг} \cdot (t_П + t_В + t_{ВИ}) \ , \qquad (3.6)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$В = \sum_i \sum_п U \, . \qquad (3.7)$$

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C,$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \qquad (4.1)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки (розділ 3.2 методичних вказівок, формула 3.8), тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Розрахунки:

Розрахунок (фіксованих) капітальних витрат

1. t =2+3+2+2+3+10+10=32 години
2. $C_{мч}$ = 0,14 *32 * 90 + 10 + 5=418
3. $З_{мч}$=32 * 418 = 13382
4. $З_{зп}$= 32 * 500 = 16000
5. $K_{рп}$ = 16000 + 13382 = 29382 грн
6. К=29382 + 5000 + 30000 = 64382 грн

Розрахунок поточних (експлуатаційних) витрат

1. $С_з$=20000*12 + 5000*12 = 300000 грн
2. $С_{ел}$ = 0,14 * 4800 * 90 = 60480 грн
3. $С_к$=20000 + 10000 + 5000 + 20000 + 300000 + 10000+20000 = 385000 грн
4. С = 385000 + 20000 + 5000 = 410000 грн

Оцінка величини збитку

1. Пп = (160000\176)*1=1000 грн

2. Пв = 2000 + 1000 + 7000= 10000 грн
3. Пви = (20000\176)*5 = 570 грн
4. U = 1000+1000+10000 = 12000 грн
5. В = 10*12000=120000 грн

Загальний ефект від впровадження системи інформаційної безпеки

E = 120000*0,5 – 410000 = -350000 грн

Коефіцієнт повернення інвестицій ROSI

ROSI = -350000\65000 = -5

Висновок:

За результатами розрахунків впровадження КСЗИ та дотримання політики безпеки не є доцільним для даного підприємства

Висновок до третього розділу:

Завдяки цьому розділу ми змогли оцінити корисність від впровадження політики безпеки на ІІЦ, та підрахувати витрати на ПБ та можливі збитки.

Список використаної літератури: