МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЛІНГВІСТИЧНИЙ УНІВЕРСИТЕТ

Кафедра менеджменту і маркетингу

Кваліфікаційна робота магістра

на тему: «ІНФОРМАЦІЙНА БЕЗПЕКА БІЗНЕСУ СУЧАСНОЇ ОРГАНІЗАЦІЇ» (на прикладі ПрАТ «Обрій Інк.»)

Допущено до захисту
«___»_____року

Завідувач кафедри
менеджменту і маркетингу
_____Тарасюк М. В.
(підпис)

Студента групи М 01-20
факультету туризму,бізнесу і психології
освітньої програми
Управління та адміністрування
бізнес-процесами
за спеціальністю 073 Менеджмент
Ітмізі Каміли Айманівни

Науковий керівник:
кандидат економічних наук,
старший викладач
Лиса С.С.

Національна шкала _____
Кількість балів _____
Оцінка ЄКТС _____

КИЇВ – 2021

ЗМІСТ

ВСТУП

З розвитком програмного забезпечення, що значно полегшило життя суспільства та, зокрема, ведення підприємницької діяльності, з'явилася інша проблема – захист інформації, що стала набагато уразливішою через велику кількість ризиків, які несуть в собі інформаційні системи. Останнім часом часто в інтернеті з'являється оприлюднена конфіденційна інформація, щобула отримана в наслідок хакерських атак, шахрайства або була просто викрадена шляхом копіювання з оригінального на сторонній носій. Для бізнесу викрадення інформації загрожує втратою репутації, конкурентоспроможності, стратегії розвитку, власних розробок, та більше того, якщо була вкрадена конфіденційна інформація клієнтів, то варто очікувати позовів до суду. Саме тому сучасні організації значно більшеприділяють уваги такому питанню як інформаційна безпека і не шкодують ресурсів для її забезпечення.

Головним принципом забезпечення інформаційної безпеки є те, що створення системи яка б могла бути на 100% захищеною від зламунеможливо. Саме тому необхідно спрямувати сили на створення механізму захисту, злам якого буде важчим та дорожчим, ніж отримана інформація.

Важливе місце у забезпеченні інформаційної безпеки суб'єктів підприємництва займає управління інформаційними ризиками. Основною особливістю тут є те, що це питання повністю покладається на підрозділи безпеки суб'єктів підприємництва і певною мірою залежить від їх можливостей. Зазвичай, управління інформаційними ризиками не інтегрується в систему управління ризиками суб'єктів підприємництва, яка є складовою процесу управління їх діяльністю. У такій ситуації роль управління саме інформаційними ризиками не виступає провідною.Подальший розвиток інформаційних технологій безумовно буде вимагати все більшої уваги до інформації взагалі і її використання у забезпеченні підприємницької діяльності. Перетворення вказаних технологій в один із

видів загроз (інтелектуальна зброя) і їх використання в конкурентній боротьбі суб'єктів підприємництва активізує пошук шляхів удосконалення інформаційної безпеки, що у свою чергу дасть поштовх змінам у її правовому регулюванні та буде сприяти підвищенню професійного рівня фахівців, залучених до забезпечення як безпеки бізнесу в цілому, так інформаційної безпеки зокрема. Тобто, є всі підстави вважати, що актуальність забезпечення інформаційної безпеки у діяльності сучасного підприємництва буде лише зростати.

Головною метою своєї роботи визначаю формування функцій та методів забезпечення інформаційної безпеки на підприємстві та беру за приклад ПрАТ «Обрій Інк.», що є компанією з організації бізнес-подорожей для співробітників крупних міжнародних корпорацій та єдиним представником в Україні компанії «American Express Global Business Travel» (надалі – AMEX GBT).

Основним об'єктом захисту є інформація клієнтів до якої належать: паспортні та інші особисті дані подорожуючих, відомості про мету та напрямок відрядження, деталі подорожі (рейси, готелі, маршрути, тощо), умови контрактів з компаніями-клієнтами та інше. Загрозами для втрати даних є:

- Різноманітні інформаційні системи
- Системи з бронювання
- Постачальники (авіакомпанії, готелі, транспортні компанії, страхові компанії та інші партнери)
- Співробітники

Таким чином, в ході даного наукового дослідження, на прикладі конкретної організації, буде створено процеси, що підвищать рівень її інформаційної безпеки, та відповідним чином їх задокументовано. Наприкінці дослідження буде проведений аналіз отриманих результатів, що допоможе визначити ефективність обраних методів.

РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ДІЯЛЬНОСТІ ПІДПРИЄМСТВ У СФЕРІ ІНФОРМАТИЗАЦІЇ

1.1. Сучасні інформаційні системи

Інформаційна система, як система управління, тісно пов'язується, як з системами збереження та видачі інформації, так і з іншої - з системами, що забезпечують обмін інформацією в процесі управління. Вона охоплює сукупність засобів та методів, що дозволяють користувачу збирати, зберігати, передавати і обробляти відібрану інформацію. Інформаційні системи існують з моменту появи суспільства, оскільки на кожній стадії його розвитку існує потреба в управлінні. Місією інформаційної системи є виробництво потрібної для організації інформації, потрібної для ефективного управління всіма її ресурсами, створення інформаційного та технічного середовища для управління її діяльністю. Інформаційна система може існувати і без застосування комп'ютерної техніки – це питання економічної необхідності [5,с.9]. В будь-якій інформаційній системі управління вирішуються задачі трьох типів:

- задачі оцінки ситуації (деколи їх називають задачами розпізнавання образів);

- задачі перетворення опису ситуації (розрахункові задачі, задачі моделювання);

- задачі прийняття рішень (в тому числі і оптимізаційні).

Автоматизована інформаційна система – це взаємозв'язана сукупність даних, обладнання, програмних засобів, персоналу, стандартних процедур, які призначені для збору, обробки, розподілу, зберігання, представлення інформації у відповідності з вимогами, які випливають з цілей організації. Сьогодні, у вік інформації, практично кожна інформаційна система

використовує комп’ютерні технології, і тому надалі під інформаційними системами надалі будемо мати на увазі саме автоматизовані [1].

Інформаційні системи включають в себе: технічні засоби обробки даних, програмне забезпечення і відповідний персонал. Чотири складові частини утворюють внутрішню інформаційну основу:

· засоби фіксації і збору інформації;

· засоби передачі відповідних даних та повідомлень;

· засоби збереження інформації;

· засоби аналізу, обробки і представлення інформації.

Різноманітність інформаційних систем з кожним роком все зростає. В залежності від функціонального призначення можна виділити такі системи: управляючі, проектуючі, наукового пошуку, діагностичні, моделюючі, системи підготовки прийняття рішення, а в залежності від сфери використання – на адміністративні, економічні, виробничі, медичні, навчальні, екологічні, криміналістичні, військові та інші.

Основними факторами, які впливають на впровадження інформаційних систем, є потреби організацій та користувачів, а також наявність відповідних засобів для їх формування. Найсуттєвіше на розвиток інформаційних систем вплинули досягнення в галузі комп’ютерної техніки та телекомунікаційних мереж.

Причини, що спонукають організації впроваджувати інформаційні системи, з одного боку обумовлюються прагненням збільшити продуктивність повсякденних робіт чи усунути їх повторне проведення, а з іншого боку бажанням підвищити ефективність управління діяльністю організації за рахунок прийняття оптимальних та раціональних управлінських рішень.

Перша причина доволі прозора і для її реалізації достатньо впроваджувати стандартизовані системи обробки інформації. Успішне функціонування організації у значній мірі залежить від вдалого керівництва, яке базується на обґрунтуванні перспективних концепцій розвитку згідно з своєчасною, достовірною та повною інформацією, яку може поставляти відповідна інформаційна система. Основне завдання інформаційної системи управління полягає у підпорядкуванні всіх внутрішніх процесів головним цілям організації. Для цього необхідно скоординувати процеси, пов’язані з діяльністю організації таким чином, щоб вони максимально забезпечували виконання поставлених задач в єдиному інформаційному полі. Тільки таким чином інформаційна озброєність організації починає безпосередньо впливати на ефективність її діяльності.

До основних напрямків автоматизації інформаційно-управлінської діяльності в організаційних структурах відносять [2]:

· автоматизацію обробки документів шляхом впровадження систем для обробки тексту, автоматизацію обміну інформацією через різноманітні види комунікацій (які включають АТС підприємства, відеотермінальні системи, локальну комп’ютерну мережу, телекопіювальні апарати, відеоінформаційні системи);

· автоматизацію діяльності менеджерів на базі комп’ютерних систем комплексних інформаційних систем, які надають допомогу в прийнятті рішень, та електронних секретарів, що дозволяє підвищити рівень організації праці менеджерів на якісно вищий щабель.

Впровадження інформаційних систем дозволяє менеджеру отримувати оперативний доступ до довільної нагромадженої інформації з тим, щоб в подальшому ефективно її використовувати для вирішення поставлених задач (в сферах аналізу маркетингу, фінансів, тощо).

Для сучасних умов характерне застосування високоефективних внутрішньо фірмових систем інформації, що ґрунтуються на використанні найновіших інформаційних технологій, зокрема єдиної локальної комп'ютерної мережі. Управлінська внутрішня інформаційна система представляє собою сукупність інформаційних процесів для задоволення потреб в інформації на різних рівнях прийняття рішень. Інформаційна система включає компоненти обробки інформації, внутрішні і зовнішні канали передачі.

Інформація, особливо її автоматизована обробка, і тепер залишається важливим фактором підвищення ефективності діяльності будь-якої організації. Важливу роль у використанні інформації відіграють способи її реєстрації, обробки, нагромадження і передачі; систематизоване збереження інформації і її видача в потрібній формі; виробництво нової числової, графічної та іншої інформації.

В сучасних умовах у великих організаціях створені і ефективно діють інформаційні системи, які обслуговують процес підготовки і прийняття управлінських рішень і вирішують наступні задачі: обробку даних, обробку інформації, реалізацію інтелектуальної діяльності з метою створення інформації. Управлінські інформаційні системи послідовно реалізують принципи єдності виробничого процесу та інформаційного процесу супроводу через застосування технічних засобів збору, нагромадження, обробки і передачі інформації в поєднанні з використанням аналітичних методів математичної статистики і моделей прогнозно-аналітичних розрахунків та інших необхідних прикладних засобів. У виробничо-господарській структурі підприємства забезпечується узагальнення інформації "знизу - вверх", конкретизація інформації "зверху - вниз", а також уніфікується інформаційний процес, спрямований на отримання науково-технічної, планової, контрольної, облікової і аналітичної інформації [4,с.33].

Підвищення ефективності використання інформаційних систем досягається шляхом наскрізної структури і сумісності інформаційних систем, які

дозволяють усунути дублювання і забезпечують багатократне використання інформації, встановлюють визначені інтеграційні зв’язки, обмежують кількість показників, зменшують обсяг інформаційних потоків, підвищують рівень використання інформації. Інформаційна система повинна підтримувати такі функції, як надання інформації (наприклад, потрібної користувачам для вирішення науково-виробничих задач) та створення найзручніших умов для її поширення (наприклад, проведення адміністративно-організаційних, науково-дослідних і виробничих заходів, які забезпечують її ефективне розповсюдження).

Сучасна інформаційна система в заданій сфері діяльності організації дозволяє забезпечити вирішення таких завдань:

1) прямий, своєчасний доступ до інформаційного продукту (точну інформацію про хід виробничого процесу в просторі та часі);

2) ефективну координацію внутрішньої діяльності та оперативне розповсюдження різноманітних повідомлень;

3) ефективнішу взаємодію із суміжниками по технологічних маршрутах за рахунок використання більш інформованих та наочних засобів відображення та передачі-прийому повідомлень;

4) виділення необхідного і неперервного часу для менеджерів всіх ланок на такі високоефективні види діяльності, як аналіз та прийняття рішень за рахунок зменшення часу на здійснення малопродуктивної діяльності;

5) використання якісно кращої технології системного аналізу та проектування оперативного управління на нижній та середніх ланках управління виробництвом.

1.2. Правила забезпечення інформаційної безпеки бізнесу

Ефективне функціонування підприємства (організації) неможливе без управління ресурсами, що використовуються для досягнення мети. Згідно з поширеними нині в управлінській літературі поглядами поняття ресурси охоплює не лише людей, капітал, сировину, а й інформацію. Зміст цілеспрямованої діяльності підприємства зводиться до виявлення необхідних ресурсів і перетворення їх у корисну продукцію. Нині не лише з теорії, а й з багаторічної практики відомо, що як природні ресурси, так і інформація для суспільства завжди обмежені. Попит на інформацію набагато перевищує можливості його задовольнити. Річ у тому, що в процесі діяльності підприємства потенційна інформація циклічно актуалізується, тобто виникає потреба в її використанні саме в той момент, коли необхідно приймати управлінське рішення, наприклад, з приводу укладання договору. Для задоволення інформаційних потреб підприємства необхідно створити оптимальну структуру з визначенням вимог, що висуваються для забезпечення інформаційної безпеки [7].

Принципово важливо, щоб інформаційна структура відповідала розподілу повноважень на підприємстві, а необхідна для вирішення завдань інформація надавалася у підрозділах не будь-кому, а лише відповідальним особам. Інформаційна структура має бути побудована таким чином, щоб задовольняти потреби усіх рівнів управління підприємством. Саме такий підхід дасть змогу правильно й оптимально вирішити проблему створення корпоративної мережі підприємства (установи).

Корпоративна мережа підприємства (установи) — це організація зв’язку в інформаційній системі корпорації через відомчу глобальну мережу, тобто обмін інформацією між кількома розміщеними на достатньо великій відстані один від одного ПК, об’єднаних локальною мережею.

Необхідно пам’ятати, що інформація суттєво відрізняється від інших видів ресурсів підприємства, а саме — її дані характеризують процеси, що протікають як у самому підприємстві, так і поза ним.

Зміст управління видами діяльності підприємства залежить насамперед від змісту і способів отримання ним інформації. Інформація, що стосується сировинних матеріалів, грошових засобів, технологічних процесів, у науковій літературі відноситься до забезпечувального фактора управління виробництвом.

Щодо іншої сторони інформації, то вона сама є особливим видом ресурсів, а тому для досягнення поставленої мети необхідно здійснювати вплив за допомогою відповідної сукупності прийомів на процеси накопичення, зберігання, поширення і використання даних на рівні підприємства. В цьому випадку інформація виступає об’єктом управління [12].

Багатоплановий підхід до інформаційних ресурсів обумовлює необхідність враховувати такий суттєвий фактор, як функціонування підприємства за умов ринкових відносин, характерною прикметою яких є боротьба між незалежними суб’єктами господарювання на ринку і гостра конкуренція товаровиробників. Боротьба за економічне виживання — закон ринку.

Забезпечення безпеки підприємства за умов ринкових відносин потребує захисту підприємницької інформації, яка в спеціальній літературі розглядається як умова, що допомагає або створює перешкоди у досягненні позитивного результату (прибутку) в господарській діяльності.

Підприємницька інформація, що створює суб’єктові вигідні умови для прийняття оперативних рішень і досягнення ефективного результату, вважається корисною. Для її захисту від сторонніх осіб, щоб не втратити очікування, як правило, застосовується комплекс методів технічного й організаційного характеру. Підприємницька інформація, що циркулює в ринково-конкурентній сфері діяльності, поділяється на організаційну, технічну, комерційну, фінансову, рекламну, є також інформація про попит і пропозицію, конкурентів, чинне законодавство, кримінальне становище,

включаючи відомості про способи, сили і засоби забезпечення безпеки інформації в корпоративній мережі підприємства тощо.

Інформація про діяльність підприємства зберігається в різних формах: у пам’яті людини, картотеках, книгах обліку, на накопичувальних пристроях.

Необхідно звернути увагу на деякі питання, пов’язані з практичним використанням технічних засобів для зберігання, видачі, обробки і пошуку інформації. Інформаційна структура має відповідати організаційній структурі управління підприємством, але необов’язково її ототожнювати. Розв’язання завдань управління направлене на об’єднання всіх видів ресурсів і потоків інформації в єдиний процес досягнення мети. Вагоме місце в технології управління посідає інформаційне поле — носії потенційної інформації, що необхідна для успішного виконання підприємством своїх завдань і функцій.

Існують взаємопов’язані технології функціонування (виробничі технології), але вони різняться за своїми характеристиками. Управлінська технологія забезпечує процес управління підприємством (установою). Для глибшого осмислення управлінської технології важливо виділити її елементи. До них належать: інформація, операція і методи здійснення управлінських технологій, персонал, обладнання, структура.

Необхідно пам’ятати, що підрозділи в складі інфраструктури підприємства пов’язані через свої властивості та завдання, що вирішуються. В цілому наявність тієї чи іншої структури з притаманними їй елементами у складі підприємства зумовлена необхідністю їх об’єднання в технологічний процес. На наш погляд, з’ясування цих обставин важливе з погляду роз’яснення значення безпеки інформації в корпоративній мережі, оскільки велика кількість підприємств має доступ до мережі Інтернет. Безперечно, це добре, з одного боку, а з іншого — усі країни світу мають доступ до внутрішньої корпоративної мережі.

Найсучаснішим обладнанням в управлінській технології є ПК (персональні комп’ютери), а також стаціонарні і рухомі засоби зв’язку. Серед них можна виділити:

- технічні засоби для обробки інформації та захисту каналів її циркулювання (фіксування, передачі, пошуку, обробки інформації);
- носії інформації — матеріальні предмети, за допомогою яких і передається інформація.

Наближеним до поняття інформаційне поле є поняття комунікаційний простір підприємства, тобто та частина середовища його функціонування, в якій він має змогу, за допомогою наявних сил і засобів, управляти інформаційними процесами, зокрема процесом актуалізації потенційної інформації. Однак комунікаційний простір підприємства може бути суттєво збільшено шляхом об’єднання з іншими інформаційними системами (наприклад, Інтернет).

Слід зазначити, що на сьогодні управлінські інформаційні технології не мають реальної альтернативи магнітному збереженню інформації.

В інформаційних системах, базовим елементом яких є комп’ютер, основна інформація зберігається на жорстких магнітних дисках. Саме у накопичувачу на жорстких магнітних дисках зберігається і з нього завантажується в оперативну пам’ять комп’ютера операційна система, інформація обробляється в процесі використання, а використана знищується.

Один з найважливіших показників — енергетична незалежність робить практично незамінним для оперативного і довготривалого зберігання великих масивів інформації. Накопичувач на жорстких магнітних дисках, як правило, називають вінчестером.

Необхідно зазначити, що в наш час великі обсяги інформації зберігаються, обробляються та передаються електронними засобами і, відповідно,

супроводжуються електромагнітним випромінюванням. Тому існує реальна можливість несанкціонованого доступу до цієї інформації за допомогою радіоперехоплення або контактного підключення до комунікацій.

Комп'ютер у режимі автономної роботи нині практично не застосовується. На автономних комп'ютерах здійснюється обробка і зберігання інформації, а за окремого підключення або за підключення до глобальної мережі Інтернет — і передача інформації (обмін інформацією).

У локальній мережі здійснюється весь обсяг роботи з інформацією: зберігання, обробка і передача.

Персональний комп'ютер є центральною ланкою в системі автоматизованої обробки інформації і привертає особливу увагу конкурентів, правопорушників і розвідувальних служб. Для отримання цінної інформації вони застосовують усі доступні засоби і методи, серед них і різноманітні типи аналізаторів, що підключаються до ліній електроживлення.

Тому найжорсткіші вимоги до захисту інформації мають встановлюватися для комп'ютерів локальної обчислювальної мережі, усі елементи якої пов'язані між собою кабельною системою. Локальну комп'ютерну мережу нині недоцільно використовувати автономно, без взаємодії з іншими мережами.

Загальними правилами забезпечення інформаційної безпеки є наступні [7]:

1. Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.
2. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати

відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

3. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.
4. Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.
5. Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися. У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.
6. Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються її власником (розпорядником).
7. У системі здійснюється обов'язкова реєстрація:
    - результатів ідентифікації та автентифікації користувачів;
    - результатів виконання користувачем операцій з обробки інформації;
    - спроб несанкціонованих дій з інформацією;
    - фактів надання та позбавлення користувачів права доступу до інформації та її обробки;
    - результатів перевірки цілісності засобів захисту інформації.

    Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в

системі (адміністратор безпеки). Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки. Реєстрація спроб несанкціонованих дій з інформацією, що становить комерційну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

8. Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.
9. Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв’язку.
10. У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;
- несанкціонованих дій з інформацією, у тому числі з використанням комп’ютерних вірусів;

- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації:

- від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить комерційну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято власником (розпорядником) інформації;
- від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах;
- від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації.

Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації. Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи. У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою. Захист інформації на всіх етапах створення та експлуатації системи здійснюється

відповідно до розробленого службою захисту інформації плану захисту інформації в системі.

План захисту інформації в системі містить:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;
- визначення моделі загроз для інформації в системі;
- основні вимоги щодо захисту інформації та правила доступу до неї в системі;
- перелік документів, згідно з якими здійснюється захист інформації в системі;
- перелік і строки виконання робіт службою захисту інформації.

Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту.

1. 3. Захист віддаленого доступу до мережі організації

Під час пандемії COVID-19 особливо актуальними стали питання організації віддаленого доступу для співробітників великої кількості компаній. Багато з організацій та їх працівників не були до цього готові, адже в компаніях переважно була відсутня можливість віддаленої роботи. Це зумовлено відволікаючими факторами, що безперечно присутні вдома у кожної людини (члени родини, домашні улюбленці, відсутність організованого робочого місця, відсутність необхідної техніки тощо). Окрім того, в умовах віддаленої роботи, набагато важче контролювати дотримання працівниками інформаційної безпеки компанії.

Віддалена робота несе в собі наступні ризики з боку захисту інформації:

- відкритий доступ до конференційних даних у членів родини або відвідувачів працівника у разі відсутності необхідної системи захисту;

- можливість втрати даних у разі пограбування, зникнення або пошкодження робочої техніки;
- недостатній захист домашньої мережі або підключення до незахищених мереж Wi-Fi може спричинити зовнішнє втручання та вилучення даних;
- віддалений доступ до інформації, може бути нестабільним та перериватися, якщо з'єднання з Wi-Fi слабке;
- пристрій або файли користувача можуть бути інфіковані програмою-вимагачем, внаслідок чого існує загроза втрати важливих корпоративних файлів;

Під час роботи в офісі більшість з цих проблем вирішує та контролює IT-персонал, застосовуючи необхідні заходи безпеки. Однак, поза цим захищеним середовищем працівникам часто доводиться справлятися з ними самостійно.

Задля підвищення рівня інформаційної безпеки необхідно дотримуватись наступних рекомендацій:

- забезпечувати віддалених працівників ноутбуками та мобільними телефонами, які призначені виключно для робочих цілей та контролюються компанією. Швидкий перехід на віддалений режим роботи може означати, що ці пристрої з’являються постфактум, але ніколи не пізно переключити виконання роботи з персонального на спеціалізований пристрій. Це особливо доречно, якщо співробітники працюють з конфіденційними або персональними даними;
- часто віддалена робота передбачає доступ працівників до інформаційних ресурсів організацій, які знаходяться у внутрішній мережі. Для цього використовують віртуальні приватні мережі (VPN), програмне забезпечення для віддаленого доступу;

- підключення до широкосмугового модему або маршрутизатора є більш практичним ніж використання Wi-Fi. Окрім того, слід заборонити працівникам використання спільного та загальнодоступного Wi-Fi;
- для захисту ваших даних використовуйте надійні паролі, що містять не менше 12 символів з маленьких і великих літер, чисел та спеціальних символів - це зменшить шанси на злам;
- багатофакторна автентифікація зараз широко доступна і її слід впроваджувати, коли масштаби віддаленої роботи збільшуються – другий фактор автентифікації слугує додатковою ланкою захисту, що унеможливлює зловмисникам доступ до конфіденційної інформації навіть при наявності викраденого пароля;
- впровадження правил з розпізнавання фішингу - вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів - логінів та паролей, досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах від імені відомих організацій. Останнім часом шахраї стали досить винахідливі у створенні фішингових листів, тому працівник навіть може отримати лист від імені свого керівника із закликом терміново перейти за посиланням у листі, але якщо придивитися до назви поштової скриньки з якої прийшов лист, то вона точно буде відрізнятися від реальної, як мінімум на один символ.

1.4. Структура служби інформаційної безпеки організації

Служба інформаційної безпеки (англ. Service of infosecurity) - організаційно-технічна структура системи забезпечення інформаційної безпеки, що реалізує вирішення певної задачі, спрямованої на протидію тій чи іншій загрозі інформаційної безпеки [10].

Дуже часто виникає питання підпорядкування Служби інформаційної безпеки в організаційній структурі Організації. На практиці найчастіше

використовується дві схеми підпорядкування СлІБ – службі безпеки Організації або директору служби ІТ.

СлІБ, як частина служби безпеки. Одна із схем, що найбільш часто зустрічається. Логіка зрозуміла – питання безпеки, значить в підпорядкування до служби безпеки. З очевидних мінусів - різні напрямки, що практично не перетинаються. Керівництво служби безпеки Організації, як правило, колишні поліцейські, військові або співробітники СБ. Вони не знають специфіки і завдань ІТ та ІБ, а звідси витікають значні проблеми в комунікаціях та прийнятті рішень щодо питань інформаційної безпеки. Ці питання ускладнюються ще й тим, що керівництво служби безпеки повинно комунікувати із керівництвом ІТ, а це призводить до повного нерозуміння один одного. Як результат - мале фінансування СлІБ , опір будь-яким нововведенням. Із позитивних моментів – великі повноваження служби безпеки Організації, що дозволяє оперативно отримувати інформацію і прискорювати прийняття рішень.

СлІБ, як частина служби ІТ. Тут зразу виникає конфлікт інтересів. Один із напрямків роботи СлІБ це, зокрема, контроль за виконанням ІТ правил, приписів і регламентів. Очевидно, що керівництво ІТ не буде зацікавленим виносити недоліки в роботі ІТ на розгляд вищого керівництва. Як результат – фінансування по залишковому принципу, ігнорування впровадження нових технологій безпеки. Із позитивних моментів – швидке впровадження нових систем, оскільки всі виконавці під рукою, прозора інтеграція систем інформаційної безпеки в інфраструктуру ІТ.

Ідеальна схема - це підпорядкування СлІБ першій особі – керівнику Організації (Правлінню або Наглядовій раді). Але така схема вимагає від першої особи виділення часу на комунікації із керівником СлІБ і необхідності вникати в питання управління інформаційною безпекою. Із позитивних моментів – окремий бюджет СлІБ, швидке прийняття необхідних рішень.

Для всіх варіантів, при обґрунтуванні місця СлІБ в структурі Організації треба враховувати те, що СлІБ безпосередньо прибуток не приносить і при розробці інвестиційних планів потрібно обґрунтовувати вигоду від нереалізованих ризиків. А чим більше ланок при узгодженні цих питань, тим важче і довше вони вирішуються, що є неприпустимим в умовах сучасних кіберзагроз.

Враховуючи вищесказане та усталені схеми управління, що прийняті в Організаціях, рекомендується вибирати компромісну схему, коли СлІБ одночасно підпорядковується першій особі і керівнику служби безпеки Організації – Рис. 1. Це дозволяє, на даному етапі управлінського розвитку Організацій, уникати частини конфліктів і забезпечувати швидкі комунікації з вищим керівництвом Організації в процесі оперативного управління системою інформаційної безпеки Організації.

Рис. 1.1 Рекомендований варіант підпорядкованості СлІБ

Відділи ІБ бізнес-підрозділів Організації адміністративно, функціонально і

методично, у даній фукціональній схемі, підпорядковуються керівнику СлІБ Організації.

Служба ІТ та структурні бізнес-підрозділи Організації підпорядковуються керівнику СлІБ в частині питань інформаційної безпеки. CISO (Chief Information Security Officer) - керівник служби інформаційної безпеки несе головну відповідальність за розробку і реалізацію політики безпеки компанії відповідно до реалізованих бізнес-процесів компанії і пріоритетного забезпечення питань неперервності бізнесу в частині питань інформаційної безпеки.

На керівника СлІБ покладаються такі ключові завдання:

- розробка політики в області ІБ, включаючи стандарти, процедури, регламенти, керівництва;
- розробка принципів класифікації інформаційних потоків і управління ними;
- аналіз ризиків, їх оцінка і прийняття;
- забезпечення персоналу всіх підрозділів настановами та знаннями по виконанню політики в області ІБ, організація відповідного навчання та інструктування;
- консультування менеджерів компанії і виконавчого персоналу в межах їх компетенції з питань інформаційних ризиків і захисту від них;
- узгодження всіх політик і регламентів з тим, щоб вони були успішно впроваджені на всіх рівнях компанії;
- діяльність у складі робочих груп або експертних рад, які оцінюють ризики при впровадженні нових технологій, модернізації виробництва, формуванні планів технічного оновлення чи інших змін бізнесу. Включення аспектів ІБ на всі етапи даних проектів;

- «Сполучна ланка» між службою якості і відділом IT/автоматизації з правом перевірки внутрішніх звітів служби якості;
- спільна робота зі службою безпеки в частині, що стосується їх обох, наприклад, науково-дослідні роботи (НДДКР) або пропускна система (бейджі, пропуски), розслідування інцидентів безпеки;
- спільна робота зі службою персоналу в частині, що стосується перевірки деяких даних при найму на роботу;
- в разі криз або надзвичайних подій в області захисту інформації брати участь разом з топ-менеджментом в управлінні кризовою ситуацією;
- забезпечення менеджменту компанії регулярними оглядами стану інформаційної безпеки, звітами про впровадження політики;
- інформаційна підтримка топ-менеджменту про зміни в законодавстві та технічні новинки, що мають відношення до інформаційної безпеки.

На службу ІБ Організації покладаються такі завдання:

- управління інформаційною безпекою та забезпечення відповідності нормативним вимогам;
- оцінка операційних ризиків Організації в частині ІБ;
- стратегічне планування розвитку ІБ Організації;
- вибір групових рішень в сфері ІБ Організації;
- забезпечення класифікації ІзОД;
- контроль за безпекою корпоративної мережі Організації;
- централізований моніторинг і запобігання несанкціонованого доступу до ІзОД;
- управління доступом до ІС Організації;

- контроль виконання стратегічної програми розвитку ІБ бізнес-підрозділами Організації;
- розробка політик і стандартів ІБ Організації;
- моніторинг подій безпеки та реагування на інциденти;
- узгодження планів розвитку і стандартів Організації з Наглядовою радою Організації.

На відділи ІБ бізнес-підрозділів Організації покладаються такі завдання:

- контроль впровадження і експлуатації систем ІБ в бізнес-підрозділах;
- управління системами ІБ в бізнес-підрозділах;
- контроль рівнів доступу до конфіденційної інформації, внесення пропозицій щодо доповнення або зміни переліку відомостей, що становлять ІзОД Організації;
- контроль за безпечною експлуатацією ІС і АСУТП;
- реагування на нештатні ситуації в ІБ;
- моніторинг і розслідування інцидентів на місцевому рівні;
- тренінг користувачів з питань ІБ.

Ці завдання можуть бути базовими при розробці організаційної структури СлІБ та формулюванні її завдань.

Організація і проведення робіт по забезпеченню ІБ Організації при її обробці технічними засобами визначаються цією Концепцією, діючими державними і міжнародними стандартами, а також іншими нормативними та методичними документами Організації.

Організація робіт по забезпеченню впровадження та підтримки працездатності засобів ІБ покладається на керівника ІТ, що здійснює

експлуатацію і супроводження ІС Організації, а методичне керівництво і контроль над ефективністю передбачених заходів захисту інформації - на керівника СлІБ.

Експлуатація ІС Організації здійснюється в повній відповідності до затвердженої організаційно-розпорядчої та експлуатаційної документації, з урахуванням вимог і положень, викладених у відповідних розділах політики безпеки.

Комплекс заходів щодо захисту інформації в Організації включає в себе наступні заходи:

- призначення ролей і розподіл відповідальності;
- розробка, реалізація, впровадження і контроль виконання планів заходів, політик безпеки та інших документів щодо забезпечення ІБ;
- підготовка користувачів і технічних фахівців до вирішення проблем, пов'язаних із забезпеченням ІБ;
- проектування, розгортання і вдосконалення технічної інфраструктури СУІБ;
- аудит ІБ Організації.

Технічна інфраструктура СУІБ призначена для вирішення наступних завдань:

- захист кінцевих точок;
- захист від руткітів і прихованих загроз;
- захист серверів;
- моніторинг і захист конфігурацій і цілісності файлів;
- захист віртуальних середовищ;
- захист мобільних пристроїв;

- захист баз даних;
- захист електронної пошти;
- забезпечення безпеки роботи з Веб;
- захист мережі і міжмережевих з'єднань;
- захист від мережевих вторгнень, DOS / DDOS атак;
- захист даних від втрати і витоків;
- сканування вразливостей серверів, кінцевих станцій і баз даних;
- сканування вразливостей веб додатків;
- аналіз та управління ризиками ІБ;
- збір та управління інцидентами ІБ;
- неперервне оцінювання відповідності стандартам і нормативним актам.

РОЗДІЛ 2. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРАТ «ОБРІЙ ІНК.»

2.1. Характеристика підприємства ПрАТ «Обрій Інк.»

ПрАТ «Обрій Інк.» - туроператор, який працює на ринку з 1996 року та засновано на засадах угоди між фізичними особами шляхом об'єднання їх майна та підприємницької діяльності.

У своїй діяльності підприємство керується Цивільним та Господарським кодексами України, законом України "Про власність", іншим законодавством України та цим Статутом.

Туристична агенція ПрАТ «Обрій Інк.» - це команда професіоналів, які допоможуть клієнту правильно вибрати відпочинок, організувати індивідуальний тур та купити квитки на літак і автобус, зекономити його час, гроші, а головне, завжди поруч, щоб надати важливу та достовірну інформацію.

Підприємство в установленому порядку може відкривати філіали, вступати в договірні відносини з іншими юридичними та фізичними особами як на території України, так і за її межами.

На сьогоднішній день партнерами компанії являються: Vassytravel, Rikki-A, Lot-ta, HolidayTravel, Landis, Tural-G (Болгарія), FlorianTravel, FurnelTravelInternational, Odegona (Польща), FortonTravel, Ostour, PilgrimTour (Словаччина), AlpinHoladay (Австрія), IscraTourOperator (Італія), більше 50 партнерів по Україні, такі як: TezTour, Turtess, AnexTour, CoralTravel, PegasTouristik, Феєрія мандрів, Пан Юкрейн, Дельта Тревел, Татур, Пілот, Проланд, СІТА, Музенідіс Трепел, Мібс трепел та ін. Також партнерами по авіаперевезеннях можна назвати: Lufthansa, Lot, AirArabia, FlyDubai, TurkishAirlines, Аеросвіт, МАУ, WizzAir, AirFrance, WindRose та ін. Також слід зазначити, що компанія „Еліта-Бізнес-Тур" користується послугами кур"єрської служби „Експрес пошта".

На даному етапі агенція ПрАТ «Обрій Інк.» виступає туроператором по організації регулярних групових екскурсійних турів в Францію.

Турагент ПрАТ «Обрій Інк.» спеціалізується не тільки на виїзному, але й на в'їзному туризмі – до України. Команда професіоналів розробила різноманітні маршрути, які цікаві і приємні в будь-який сезон року. Клієнт отримує повний набір послуг, включаючи замовлення мандрівки, бронювання квитків і готелів, екскурсій тощо.

Предметом діяльності туристичної агенції ПрАТ «Обрій Інк.» є:

1) обслуговування іноземних туристів і продаж поїздок іноземним туристам на комерційній основі, розробка і впровадження нових туристичних маршрутів;

2) організація та надання послуг гідів-перекладачів, забезпечення зустрічі, екскурсійне обслуговування, організація театрально-видовищних та інших заходів, транспортні послуги туристам;

3) здійснення на договірній основі бронювання транспортних, готельних та інших послуг;

4) візова підтримка (заповнення візових анкет, збір документів для подачі в консульство, запис на співбесіду у візовий центр, консульство таін.);

5) надання посередницьких послуг в межах країни та за її межами;

6) здійснення заходів із підвищення економічної ефективності закордонного і внутрішнього туризму, якості та конкурентоспроможності наданих послуг при найменших видатках;

7) продаж сувенірів, посередницька діяльність;

8) операції з нерухомістю, комерційні фірми та посередницькі послуги, брокерська і дилерська діяльність;

9) надання агентських, рекламних , інформаційних і представницьких послуг;

10) робота у галузі громадського харчування (експлуатація ресторанів, кав'ярень і їдалень);

11) індустрія розваг (парки, атракціони, концертна діяльність, театри).

Метою створення є розширення асортименту туристичних послуг на ринку, організація надійного і якісного обслуговування туристів, всебічне задоволення попиту на туристичний продукт.

Організаційні структури управління туристичними фірмами відрізняються великою різноманітністю і залежать від багатьох факторів. До них можуть бути віднесені, зокрема, розміри фірм (середня, дрібна, велика), профіль фірми (спеціалізація на одному конкретному напрямку або декількох напрямків), і пр.

Для ПрАТ «Обрій Інк.» є характерна функціональна організаційна структура управління, представлена на рис. 2.1

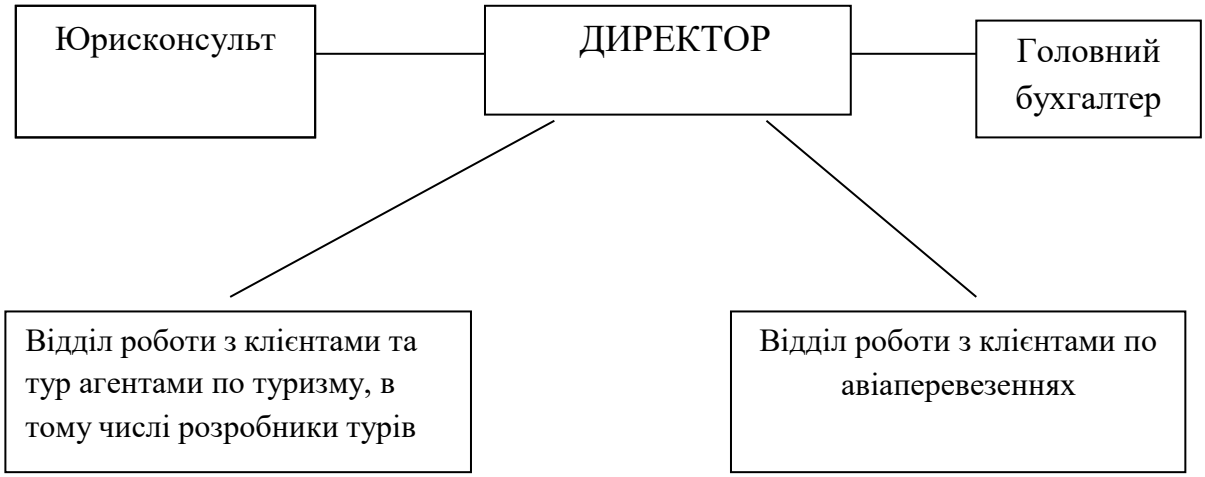

Рис. 2.1 Організаційна структура управління ПрАТ «Обрій Інк.»

Управління товариством здійснює керівник організації на контрактній основі. Серед його основних обов'язків є те, що він визначає стратегію діяльності фірми, веде туристичну документацію, укладає договори з клієнтами та партнерами, контролює введення бухгалтерської звітності, представляє інтереси агенції у державних та громадських організаціях, тощо.

Відділ роботи з клієнтами та турагентами по туризму напряму працює з турагентами – товариствам, яким продає тури, що пропонує організація.

Менеджери цього відділу займається розробкою турів (турпродукту) та забезпечують процес виконання тур продукту (комплекс туристичних послуг, необхідних для задоволення потреб туриста під час його подорожі) та мають безпосередній контакт з клієнтами (туристами

Відділ роботи з клієнтами по авіа-перевезеннях займаєтьсябронюванням та продажем авіаквитків.

Функції головного бухгалтера: він несе відповідальність за формування облікової політики підприємства, стан та ведення бухгалтерського обліку, своєчасність і достовірність бухгалтерської звітності, тощо.

Юрисконсульт, зокрема в межах своїх повноважень, здійснює контроль за законністю наказів і розпоряджень організації; бере участь у складанні проектів договорів та угод, що укладаються з юридичним чи фізичним особами, надає правову допомогу працівникам свого підприємства, візує окремі ділові документи.

Аналізуючи фінансові результати ПрАТ «Обрій Інк.» (табл.1.1) протягом досліджуваного періоду спостерігається суттєве підвищення собівартості продукції. Його причиною є зростання транспортних витрат, витрат на оплату праці, рекламу, обладнання тощо. Позитивною динамікою характеризується чистий дохід від реалізації, який протягом досліджуваного періоду зріс від 32,69% порівняно з 2018 (рис. 2.2).

Показник	**Рік**			Абсолютне відхилення, ±	Відносне відхилення, %
	2018	**2019**	**2020**	2020 / 2018	2020 / 2018
1	**2**	**3**	**4**		
Чистий дохід від реалізації продукції	208746	246644	276981	68235	132,69

Валовий дохід	124904	150745	171875	46971	137,61
Собівартість продукції	-88159	-100952	-111265	-23106	126,21
Фінансовий результат до оподаткування	15956	22782	6659	-9297	41,73
Чистий фінансовий результат	13187	18252	4277	-8910	32,43

Таблиця 1.1 - Динаміка фінансових результатів ПрАТ «Обрій Інк.» за 2018-2020 рр., тис. грн.

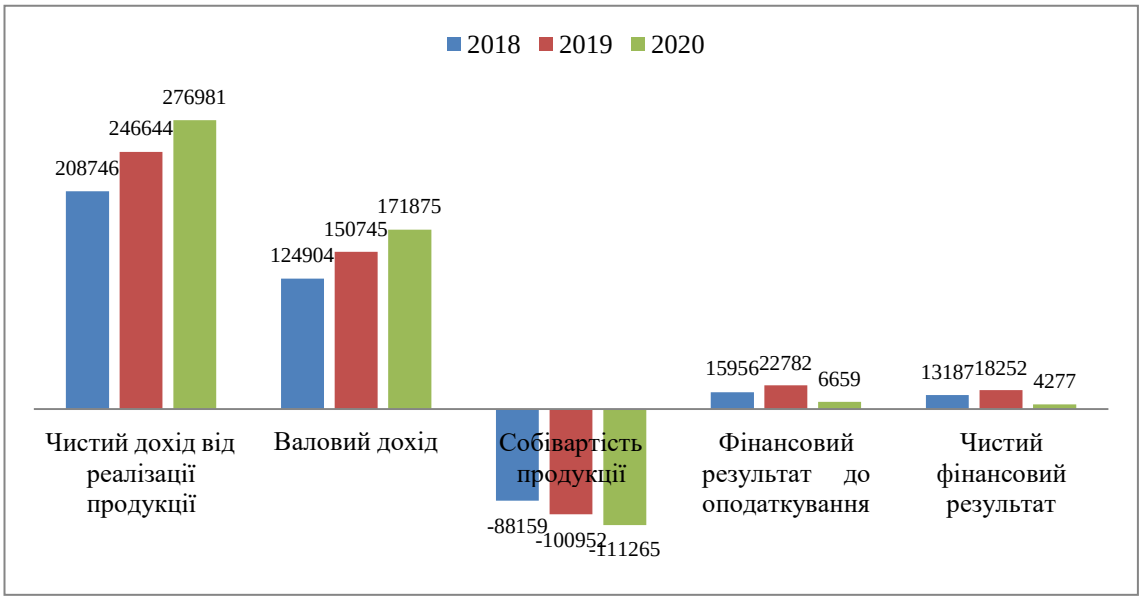

Рис. 2.2 - Показники фінансових результатів ПрАТ «Обрій Інк.» за 2018-2020 рр.

На сьогоднішній день по більшості економічних показників (рентабельність, ліквідність, платоспроможність) ПрАТ «Обрій Інк.» можна вважати цілком процвітаючим і стійким у фінансовому плані.

Логістика є одним з важливих інструментів ефективного менеджменту кожного підприємства. Саме завдяки здійсненню логістичних функцій планується, реалізується і контролюється ефективний і продуктивний потік товарів, їх запаси, сервіс і пов'язана інформація від їх зародження до поглинання (споживання) з ціллю задоволення вимог споживачів .

В ПрАТ «Обрій Інк.» логістична діяльність представлена тільки вдалим розміщенням компанії, де клієнти змогли б швидко дістатися на машині чи супутньому транспорті.

Ми пропонуємо ПрАТ «Обрій Інк.» використання можливостей Інтернету як перспективного каналу для побудови ефективної комунікації з потенційною клієнтурою. Хоча даний напрямок комунікаційного зв’язку дає можливість юридичним фірмам м. Кривому Розі та області створити ефективну систему просування власних юридичних послуг не тільки з потенційними клієнтами на регіональному рівні, а й в подальшому створити передумови для охоплення клієнтури далеко за його межами.

Узагальнюючи дослідження, ми пропонуємо такий алгоритм формування стратегії логістики для ТОВ «ЦЕПСП» , що складається з трьох етапів:

1. Прийняття корпоративної бізнес-стратегії підприємства з визначенням показників вимірювання її виконання.

2. Розроблення логістичної стратегії.

– Визначення напрямів і функціональних сфер розвитку логістики, скерованих на виконання стратегії підприємства.

— Визначення показників вимірювання виконання стратегій логістики.

– Проведення SWOT-аналізу реалізації логістичних стратегій. З’ясування сильних і слабких сторін підприємства, необхідності залучення додаткових

ресурсів тощо. Визначення зовнішніх можливостей і загроз, наприклад, зміна ринкової кон'юнктури, стратегій провідних конкурентів, тощо.

– Координація логістичної стратегії зі стратегіями маркетингу.

– Розроблення системи мотивації, спрямованої на виконання стратегії логістики.

3. Упровадження стратегії логістики.

– Створення системи моніторингу і контролю.

Запропоновані логістика й алгоритм формування стратегії розвитку логістики для ПрАТ «Обрій Інк.» складається з трьох етапів. Для формування та розвитку логістичної інфраструктури ПрАТ «Обрій Інк.» рекомендовано приділити увагу розміщенню підприємства і доступними шляхами.

Реалізація турпродукту здійснюється безпосередньо і через турагентства на підставі агентських договорів.

У туристичному агентстві ПрАТ «Обрій Інк.» застосовуються досить різноманітні способи стимулювання збуту.

Серед них знижки з ціни туру на гарячі путівки.

При покупці туру з максимальною тривалістю компанія надає додаткове безкоштовне обслуговування протягом одного-трьох днів.

Після придбання десяти турів надається безкоштовна поїздка.

При купівлі будь-якого туру компанія дарує від 2 до 4 днів безкоштовного відпочинку в заміському клубі «Богема».

Проводяться лотереї для всіх клієнтів з призом у вигляді безкоштовної поїздки.

Покупцям турів роздають фірмові сувеніри (ручки, блокноти, футболки, кепки, дорожні сумки).

Особлива увага приділяється обслуговуванню постійних клієнтів туристичного агентства: подарунки, дорогі сувеніри, розсилки поздоровлень

з нагоди свят, урочистих дат і т.д. Також в компанії прийнято урочисте вшанування ювілейних (1, 10, 100 - тисячних) туристів. Вручення їм цінних подарунків або надання значних пільг при покупці туру.

Основними цілями стимулювання по відношенню до споживача є:

- збільшення числа покупців;
- збільшення обсягу покупок одним клієнтом; прихильність покупців до торгової марки.

Для того, щоб реклама була ефективною, вона повинна бути витримана в фірмовому стилі, подана професійно і грамотно. Тому насичення сторінок мережі Інтернет має суворо контролюватися рекламною кампанією. Також на всій рекламної продукції (візитні картки, бланки і т.д.) повинен міститися електронну адресу компанії (URL).

Рекламні засоби	2019				2020			
	План	Факт	Абсолютне відхилення (+/-)	Відносне відхилення, %	План	Факт	Абсолютне відхилення (+/-)	Відносне відхилення, %
Зовнішня реклама	650	600	-50	92,3	700	700	-	100
Телереклама	400	330	-70	82,5	600	-	-600	-
Промоакції	100	120	20	120	150	200	50	133
Реклама в Internet	30	20	-10	66,7	30	20	-10	66,7
Презентації	100	120	20	120	200	310	110	150
Друкован	300	420	120	140	300	315	15	105

а реклама								
Разом	1580	1610	30	102	1980	1545	-435	78

Таблиця 2.2 Аналіз використання різних рекламних засобів в ПрАТ «Обрій Інк.»

Одним з найбільш недорогих, але при цьому дуже ефективнихрекламних засобів є промоушен. Необхідно відзначити, що збільшення обсягів продажів, ступеня інформованості покупців про продукцію і фірмі в це- лом сприяє проведення різних акцій, вручення подарунків, розіграш призів, консультація фахівців.

ПрАТ «Обрій Інк.» не допускає ситуації, коли рекламованого товару не виявляється в продажу, або характеристики послуги не відповідають дійсності. Компанія строго стежить за дотриманням логічного ланцюга реклами товарів. У свою чергу менеджери з продажу фірми ТОВ «Тімбервуд Юей» намагаються надати потенційному клієнту всю необхідну йому інформацію про туристичні послуги.

На рисунку 2.3 наведені показники використання рекламних засобів ПрАТ «Обрій Інк.»

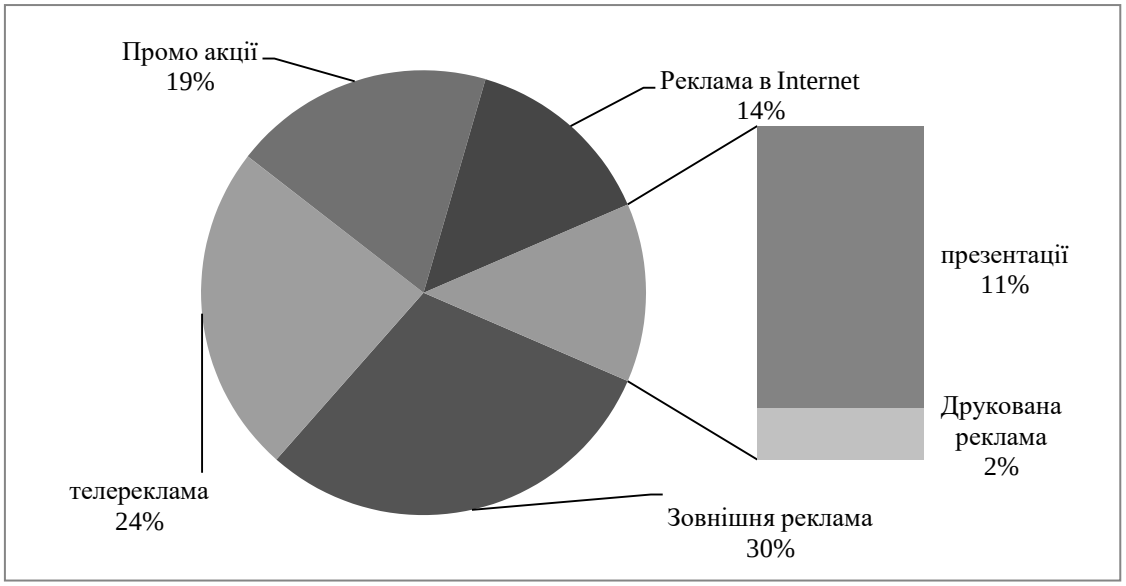

Рисунок 2.3 - Показники використання рекламних засобів ПрАТ «Обрій Інк.»

Виходячи з даних діаграми можна зробити висновок, що більшу частину коштів компанія ПрАТ «Обрій Інк.» вкладає в телерекламу і в зовнішню рекламу. Даний медіаканал є найефективнішим і «Дорогим» серед всіх інших. Інші показники використання рекламних засобів можна оцінити виходячи з даних діаграми.

Проаналізувавши рекламну діяльність на підприємстві можна зробити наступні висновки - вся рекламна діяльність узгоджується з організацією і діяльністю рекламної служби міста (журнали, газети, телеканали), де фірма і розміщує свої рекламні повідомлення.

Таким чином, навіть в кризових і важких економічних умовах фірма ПрАТ «Обрій Інк.» приділяє своїй рекламній діяльності велику увагу. Однак очевидно, що підвищення ефективності рекламної діяльності фірми можливо через розробку рекламної стратегії компанії ПрАТ «Обрій Інк.».

Ефективність рекламних кампаній керівництво ПрАТ «Обрій Інк.» оцінює шляхом проведення маркетингових досліджень, адже тільки думка споживачів даної продукції може бути об’єктивною оцінкою того, що зроблено.

Одним із головних завдань менеджменту ПрАТ «Обрій Інк.» є визначення мети, для досягнення якої формується, функціонує й розвивається дана турагенція.

Менеджери досліджуваної турагенції при формулюванні місії акцентують увагу на трьох її основних елементах:

- розробка та виробництво друкованої продукції для поширення у точках продажу та для роздачі потенційним клієнтам (постерів, вивісок);

- розробка візуального оформлення презентацій для допомоги продажу, веб-контенту, опис процесу продажу для відповідних спеціалістів, внутрішній опис продукту, безкоштовний опис продукту для клієнтів.

До інновацій в туризмі слід відносити перш за все ті нововведення, які супроводжуються: відновленням і розвитком духовних та фізичних сил туристів; якісно новими змінами турпродукту; підвищенням ефективності функціонування інфраструктури туризму; підвищенням ефективності процесів формування, позиціонування та споживання туристичних послуг; прогресивними змінами факторів виробництва [3].

Незважаючи на швидкий розвиток інформаційних технологій, телекомунікацій і електронної торгівлі, більшість туристських організацій тільки в середині 1990- х рр. стали активно використовувати Інтернет у своїй діяльності.

Інтернет дозволяє туристським організаціям, без більших витрат одержати доступ до більших груп споживачів з метою передачі конкретної інформації про пропоновані продукти й про організацію їх продажів; надійно поширювати повну й докладну інформацію про свою діяльність; швидко й ефективно ухвалювати заявки клієнтів і робити бронювання необхідних послуг; скоротити витрати на виробництво й поширення друкованої продукції; прискорити й спростити взаємодія з партнерами на ринку.

На мою думку, класифікувати інновації в ПрАТ «Обрій Інк.» слід наступним чином:

I. Продуктові інновації

1. Створення нових туристичних продуктів.
2. Освоєння нових сегментів туристичного ринку.
3. Освоєння нових туристично-рекреаційних територій.
4. Залучення до туристичного сегменту нових видів ресурсів.

II. Управлінські інновації

1. Нові методи реалізації маркетингового циклу в туризмі.

III. Сервісні інновації

1. Впровадження передових методів навчання, підготовки та перепідготовки працівників.

IV. Технологічні інновації

1. Впровадження комп'ютерних технологій в систему бронювання і резервування готелів, авіаквитків.

2. Розробка нових видів матеріально-технічного забезпечення туристичного обслуговування, покращення якості послуг.

3. Нововведення в системі транспортного обслуговування, що будуть спрямовані на підвищення комфортності та скорочення часу трансферу туристів до курортної зони.

Такі новації ПрАТ «Обрій Інк.» використовує в методах управління організацією. Багато інших новацій пропонують партнери з закордону, але вже вирішення чи користуватися ними, чи вводити їх в обхід фірми визначає директор. Також директор може підняти це питання на зборах засновників, або ж дізнатися думки колективу. Так як, колектив в ПрАТ «Обрій Інк.» - молодий, директора часто цікавить думка своїх менеджерів, їх позиція щодо нововведень, а також пропозиції.

Регулювання ЗЕД в ПрАТ «Обрій Інк.» здійснюється для забезпечення збалансованості економіки та рівноваги внутрішнього ринку України, стимулювання прогресивних структурних змін в економіці та створення найсприятливіших умов для залучення економіки нашої держави до системи світового поділу праці та наближення її до ринкових структур розвинених країн світу.

У своїй діяльності ПрАТ «Обрій Інк.» керується такими законодавчими та нормативними актами:

1. Законом України «Про зовнішньоекономічну діяльність» [9], крім того, у відповідних сферах регулюючу роль відіграють й інші Закони України: «Про чинність міжнародних договорів на території України», «Про іноземні інвестиції», «Про міжнародний комерційний арбітраж», «Про режим іноземного інвестування» тощо.

2. Законом України «Про порядок здійснення розрахунків в іноземній валюті», який описує особливості у регулюванні терміну

здійснення платежів по операціям та порядку купівлі або продажу іноземної валюти та здійснення розрахунків з нерезидентами [10].

3. Податковою Службою України, експорт товарів за межі митної території України обчислюється за нульовою ставкою за умови, якщо експорт підтверджується належно оформленою вантажною митною декларацією, яка подається в Податкову службу України.

4. Митним Кодексом, який є основним нормативно-правовим актом, що регулює зміст та порядок розрахунку митної вартості [11].

Це основний перелік державних законодавчих та нормативних актів, якими у своїй діяльності керується ПрАТ «Обрій Інк.»

2.2. Політика інформаційної безпеки ПрАТ «Обрій Інк.»

Всі дані/інформація в компанії поділяються на такі види:

- Публічна інформація
- Внутрішня інформація
- Закрита, конфіденційна інформація
- Секретна інформація
- Зовнішня інформація

Публічна інформація:

- Інформація, відкрита для доступу до будь-якого співробітника
- Може бути надіслана, передана на зовнішні ресурси
- Не потребує особливого рівня прав доступу

Внутрішня інформація:

- Інформація, що супроводжує та підтримує внутрішні бізнес процеси
- Може бути поширена між співробітниками компанії
- Може бути надіслано третій стороні, за умови підписання договору про нерозповсюдження інформації

- Більшість інформації у компанії класифікується як внутрішня інформація

Закрита, конфіденційна інформація:

- Інформація, неправильне використання, якою може скомпрометувати компанію в галузі конкурентних переваг, конфіденційності даних співробітників та клієнтів, юридичних та фінансових статусів.
- За замовчуванням до закритої інформації належать персональні дані

Секретна інформація:

- Інформація, неправильне використання, яка може серйозно скомпрометувати компанію в галузі конкурентних переваг, юридичного та фінансового статусу.
- За умовчанням це класифікація для авторизаційних даних, таких як пароль, логін, код PIN.
- Перед надсиланням іншій стороні Закритої, конфіденційної або Секретної інформації рекомендується скористатися засобом шифрування даних.

До зовнішньої інформації належать паспортні дані клієнтів, інформація про візи, банківські картки, деталі подорожей, накази на відрядження та будь-яка інша інформація, що надається клієнтом в рамках співпраці для організації подорожей. Більш детально про те, як збирається, зберігається та обробляється інформація про клієнта, можемо бачити у таблиці 2.3, що є витягом з політики конфіденційності компанії.

Яку інформацію збирає компанія	Компанія збирає інформацію про клієнта, що є необхідною для надання послуг згідно з його запитом.

Як компанія використовує інформацію про клієнта	Компанія використовує інформацію клієнта, щоб надавати наші послуги, обробляти платежі, керувати нашими веб-сайтами та мобільними додатками, продавати продукти та послуги, створювати бізнес-інсайти та дотримуватись законодавства.
Як компанія ділиться інформацією	Компанія отримує інформацію від клієнта, його роботодавця або спонсора подорожей, який є корпоративним клієнтом, і передає інформацію афілійованим особам, постачальникам туристичних послуг. Компанія не продає і не передає інформацію третім сторонам, щоб вони могли самостійно продавати власні продукти чи послуги безпосередньо клієнту.
Як компанія захищає та зберігає інформацію клієнта	Компанія використовує розумні адміністративні, технічні та фізичні заходи безпеки, щоб захистити особисту інформацію клієнта від несанкціонованого доступу та використання.
Міжнародні перекази	Компанія передає інформацію клієнта за межі відповідної країни, згідно законодавства. Щоб захистити інформацію, міжнародні передачі здійснюються відповідно до угод про передачу даних та інших заходів захисту.

Таблиця 2.3 Витяг з політики конфіденційності ПрАТ «Обрій Інк.»

Яку саме інформацію ПрАТ «Обрій Інк.» збирає про клієнта:

- Інформація про обліковий запис – якщо клієнт зв’язується з компанією, реєструється у на сайті або отримує послуги, то ПрАТ «Обрій Інк.»

збирає інформацію про дану особу. Це може включати ім’я, адресу електронної пошти, номери телефонів, роботодавця та фізичні адреси. За необхідності, можуть бути запрошені номер паспорта, номери візи, стать і дата народження мандрівників. Якщо бронюються подорожі для супутників, може біти зібрана подібна інформація про них. Інформація облікового запису надходить у профіль мандрівника, де зберігається інформація, необхідна для бронювання подорожі та надання послуг. Клієнт може надати більше інформації для фіксації у профілі мандрівника, включаючи облікові дані частих мандрівників, державні ідентифікатори та контактну інформацію для екстрених випадків;

- Інформація про подорожі - якщо клієнт бронює подорож , компанія збирає деталі (наприклад, місце прибуття та вильоту, деталі про авіакомпанію, готель та оренду автомобіля) та будь-яку іншу інформацію, необхідну для завершення бронювання;
- Платіжна інформація - для оплатити бронювання та інших транзакцій, компанія збирає інформацію про платіжну картку та інші дані, необхідні для обробки платежів;
- Дані пристрою – компанія збирає інформацію про те, як клієнт отримує доступ до послуг, включаючи IP-адресу комп’ютера та інформацію, яку можна отримати завдяки їй (наприклад, про постачальника Інтернету та загальне географічне розташування), унікальний ідентифікатор вашого пристрою та іншу технічну інформацію. Ми також збираємо інформацію про те, як ви використовуєте наші веб-сайти та мобільні додатки.

Яким чином ПрАТ «Обрій Інк.» використовує зібрану інформацію:

- Пропонує клієнтам туристичні продукти та послуги - використовує інформацію для бронювання подорожей, організації зустрічей та подій, підготовки маршрутів і рахунків-фактур, спілкування з клієнтом щодо

його подорожей чи продуктів та послуг компанії, надання послуг клієнтам та керування клієнтським обліковим записом;

- Надає продукти та послуги корпоративним клієнтам – використовує інформацію для виконання угод з клієнтом, його роботодавцем або спонсором подорожей, повідомляє про продукти та послуги, та допомагає їм забезпечити відповідність їхнім політикам;
- Обробляє платежі – використовує інформацію для обробки транзакцій і надання відповідного обслуговування клієнтам;
- Керує веб-сайтами та мобільними додатками - використовує дані пристрою для моніторингу та покращення продуктивності та вмісту послуг, надання оновлень та аналізу тенденцій;
- Покращує бізнес – використовує інформацію для дотримання політики та процедур компанії, для бухгалтерських та фінансових цілей, для виявлення або запобігання шахрайству чи злочинної діяльності, для виконання, аналізу та покращення послуг та інших випадків, як того вимагає закон.

Для захисту інформації була розроблена політика інформаційної безпеки, усі співробітники компанії, включаючи менеджерів, несуть персональну відповідальність за дотримання цієї політики. Основним принципом використання інформації в компанії є обмеження права доступу до інформації у відповідність до виробничої необхідності та функцій співробітників.

Усі співробітники компанії зобов'язані:

- Використовувати інформацію відповідно до цієї політики, та у відповідність до інших корпоративних політик та стандартів щодо забезпечення збереження та конфіденційності інформації компанії;

- Нести персональну відповідальність за збереження комп'ютерного обладнання та програмного забезпечення до нього, що знаходяться в їх безпосередньому використанні;
- Своєчасно інформувати менеджерів та відповідні служби компанії про випадки несанкціонованого використання інформації та комп'ютерного обладнання іншими особами, а також про випадки крадіжки інформації, обладнання та програмного забезпечення. Також необхідно негайно доповідати до відділу інформаційних систем про випадки дії вірусів;
- Зберігати у таємниці паролі доступу до ресурсів інформаційної мережі
- Не проводити копіювання файлів, документів, програмного забезпечення та інших інформаційних ресурсів компанії на знімні носії без отримання письмового дозволу від Менеджера відділу.
- Заборонено виведення на друк конфіденційної інформації та винесення роздрукованих документів за межі офісу компанії.
- Будь-які роздруковані документи мають бути зібрані з принтера і у разі відсутності у їх необхідності повинні бути видалені без можливості їх відновлення.

Менеджери всіх рівнів зобов'язані:

- Забезпечити впровадження та виконання процедур захисту інформації компанії;
- Слідкувати за тим, щоб співробітники компаній, які надають послуги ПрАТ «Обрій Інк.», та мають доступ до інформації компанії, розуміли суть підписаної ними угоди про нерозголошення конфіденційної інформації
- Визначати рівні та права доступу співробітників до систем та баз даних компанії;
- Навчати співробітників своїх відділів з тим, щоб забезпечити їхню відповідальність щодо захисту інформації компанії;

- Заздалегідь інформувати відділ інформаційних систем про зміни в кадровому складі відділу;
- Приймати відповідні дисциплінарні заходи у разі недотримання співробітниками цієї політики.
- Проводити шифрування даних перед надсиланням інформації класу закрита, конфіденційна та/або секретна.

Відповідальність відділу інформаційних систем:

- Стежити за неухильним виконанням цієї політики та інших процедур компанії захисту інформації;
- Здійснювати встановлення рівнів та прав доступу співробітників до систем та баз даних компанії;
- Забезпечення всеосяжного захисту програм та баз даних компанії.
- Проводити інструктаж щодо роз'яснення правил використання електронної пошти.
- Проведення регулярного аудиту комп'ютерного обладнання та програмного забезпечення до нього, що перебуває у користуванні співробітників, на відповідність до цієї політики.
- Проводити вибірковий моніторинг роботи співробітників на персональних комп'ютерах компанії та програмному забезпеченні компанії.
- Відстежувати використання працівниками робочих персональних комп'ютерів, телефонів, мобільних пристроїв, програмного забезпечення, оргтехніки та каналів зв'язку.

Відповідальність відділу персоналу:

- Інформувати новоприйнятих на роботу співробітників про політику компанії щодо захисту інформації компанії;
- Вживати відповідних дисциплінарних заходів у разі недотримання співробітниками реальної політики.

- Слідкувати за тим, щоб співробітники компаній, які надають послуги ПрАТ «Обрій Інк.», та мають доступ до інформації компанії, підписували угоду про нерозголошення конфіденційної інформації.

Усі співробітники компанії зобов'язані дотримуватися таких правил:

- Кожен користувач повинен мати в системі унікальний Логін/ID, який включає його ім'я, а також рівні доступу до інформації. Логін/ID співробітника є конфіденційною інформацією та не підлягає розголошенню.
- При додаванні користувача до системи має бути заповнена відповідна форма, яка засвідчується менеджером користувача. Тільки на підставі цієї форми відділ інформаційних систем може ввести користувача до системи. Дана форма є також офіційною заявою користувача про те, що він/вона знайома з справжньою політикою компанії захисту інформації, і зобов'язується суворо її виконувати.
- Доступ до інформації має бути організований за принципом виробничої потреби.
- Доступ до комп'ютера має бути закритий паролем.
- Паролі доступу до баз даних повинні зберігатися в суворій таємниці та не розголошуватись співробітниками.
- Комп'ютери та інше обладнання, що є власністю компанії, повинні бути оснащені лише програмним забезпеченням, закупленим, розробленим або дозволеним для використання компанією. Встановлення програмного забезпечення, яке не є ліцензійним і не є власністю компанії, суворо заборонено.
- Диски на всіх комп'ютерах повинні бути деактивовані. Тільки на підставі запиту менеджера у зв'язку з виробничою необхідністю співробітнику надається право користування дисководом. Цей співробітник несе персональну відповідальність за захист інформації

компанії, а також має особисто вживати заходів щодо захисту програмного забезпечення від дії вірусів.

- Співробітники компанії (за винятком співробітників відділу інформаційних систем) не мають права видаляти, копіювати, переносити ліцензійне програмне забезпечення на інші комп'ютери.
- Вся інформація, яка має виробничу та фінансову цінність, повинна зберігатися на мережному файловому сервері з метою забезпечення резервного копіювання.
- Користувачі портативних комп'ютерів несуть персональну відповідальність за фізичну безпеку обладнання та програмного забезпечення. На даний вид комп'ютерів поширюються всі положення цієї політики. Забезпечення даних комп'ютерів має відповідати всім стандартам захисту інформації компанії.
- Відділ інформаційних систем відповідає за впровадження та підтримку регулярної процедури резервного копіювання даних, з метою безперебійної роботи компанії.

Співробітникам компанії, користувачам електронної пошти суворо забороняється:

- Пересилати інформацію, що має виробничу та фінансову цінність будь-яким зовнішнім адресатам, які не є співробітниками компанії ПрАТ «Обрій Інк.».
- Використовувати мережу для широкомасштабного особистого листування, обміну посланнями та документами, що не мають відношення до роботи.
- Використовувати електронну пошту для надсилання зовнішньої кореспонденції, яка не має відношення до роботи, на приватні та робочі адреси знайомих.

- Надсилати, отримувати, переглядати та зберігати різного роду екранні заставки, ігри, комп'ютерні віруси та образливі матеріали, як усередині компанії, так і у листуванні із зовнішніми партнерами.
- Зберігати такі матеріали на носіях, які є власністю компанії.
- Використання файлів, документів, програмного забезпечення та інших ресурсів компанії під час використання браузерної публічної пошти.

Співробітники відділу інформаційних систем, періодично (але не рідше 1 разу на рік) проводять аудит користувальницьких станцій щодо відповідності цій політиці та іншим стандартам компанії із захисту інформації. Співробітники цього відділу мають право не повідомляти користувачів про дати майбутніх аудиторських перевірок.

У разі виявлення під час перевірок фактів порушення цієї політики співробітники відділу інформаційних систем складають письмовий звіт на адресу безпосереднього менеджера користувача, з копіями Генеральному директору та у відділ персоналу.

У разі регулярного порушення цієї політики, до співробітника можуть бути вжиті заходи дисциплінарного порядку, аж до припинення співробітництва чи звільнення.

У компанії повинні бути дотримані такі заходи безпеки щодо фізичної безпеки комп'ютерів компанії та процедури утилізації технологічного обладнання:

- Заборонено розміщення робочих ПК у приміщеннях, що не охороняються.
- Усі співробітники повинні завершувати роботу персональних ПК та лептопів компанії після завершення робочого дня.

- Забороняється розміщувати записаний пароль до комп'ютерів у виді будь-якого співробітника місці (на моніторі, поруч із ПК, інше).
- Кожен співробітник повинен проводити блокування свого ПК перед виходом з робочого місця на короткий термін (Windows+L або пуск – Завершення роботи – Блокувати).
- Співробітники відділу інформаційних систем проводять налаштування прав доступу та дії для кожного користувача ПК окремо. Працювати під користувачем Адмін заборонено всім, окрім співробітників відділу інформаційних систем.
- Заборонено працювати під одним і тим самим користувачем на різних ПК одночасно.
- Розміщення та переміщення робочих стаціонарних ПК дозволено лише співробітникам відділу інформаційних систем.
- Якщо ПК був пошкоджений, втрачений, вкрадений або іншим чином недоступний для звичайної виробничої діяльності, користувач, призначений для роботи на цьому ПК, повинен негайно поінформувати співробітника відділу інформаційних систем, системного адміністратора компанії.
- До технологічного обладнання відноситься стаціонарний ПК, планшет або ноутбук, принтер, копіювальний апарат, монітор, сервер, телефон, мобільний телефон, дисковий накопичувач або будь-який пристрій зберігання, мережний комутатор, маршрутизатори, бездротова точка доступу, акумулятор і т.д. .
- Коли технологічний актив досяг кінця терміну служби, співробітник відділу інформаційних систем повинен замінити його на новий або аналогічний, для продовження виконання поточних бізнес-процесів користувача.
- Співробітник відділу інформаційних систем повинен надійно очистити середовище зберігання даних на устаткуванні відповідно

до поточного передового досвіду. Усі дані, включаючи файли та ліцензійне програмне забезпечення, повинні бути видалені.

- Все списане з експлуатації обладнання повинно бути утилізовано відповідно до чинних правових норм та процедур.

Віддалений доступ до корпоративної мережі та пошти можливий лише авторизованому колу співробітників.

Для підключення до корпоративної мережі слід використовувати верифікований VPN клієнт Cisco, попередньо встановлений на робочий стіл, з ключем та паролем.

Якщо співробітнику потрібен віддалений доступ до корпоративної мережі та пошти, його Менеджер повинен розмістити відповідну заявку до відділу інформаційних систем.

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ДЛЯ ПОКРАЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРАТ «ОБРІЙ ІНК.»

3.1. Виявлені проблеми із забезпечення інформаційної безпеки ПрАТ «Обрій Інк.»

У 2001 році компанія «Обрій Інк.» стала представником American Express Global Business Travel в Україні, що накладає на неї зобов'язання дотримуватись всіх вимог з інформаційної безпеки, встановлених міжнародним партнером. Виходячи з того, що в Україні технології із захисту інформації значно відстають від американських колег, компанія знаходиться тільки на шляху до втілення всіх необхідних заходів.

American Express Global Business Travel цінує всі види інформації, так як інформація є одним із драйверів бізнесу. Ключовим активом, який допомагає захистити програма інформаційної безпеки, є дані.

Приклади даних, які необхідно захищати:

- Інформація про продукт, включаючи проекти, плани, патентні заявки, вихідний код та креслення
- Фінансова інформація, включаючи оцінки ринку та власні фінансові записи компанії
- Інформація про клієнтів, включаючи конфіденційну інформацію, яку компанія зберігає від імені клієнтів або подорожуючих

American Express Global Business Travel вимагає, щоб партнери захищали дані так само, як і вони. Саме через це, вони щороку проводять навчання для всіх свої співробітників та співробітників компаній-партнерів.

Компанія оцінює своїх партнерів за нижчезазначеними критеріями:

1) Управління ризиками інформаційної безпеки

- Призначені власники процесів та власники інформації, які визначають, оцінюють, пом’якшують та керують інформаційними ризиками, пов’язаними з бізнес-процесами, допоміжними технологічними рішеннями та іншими інформаційними ресурсами
- Офіційний, документований процес оцінки ризиків інформаційної безпеки, який включає нагляд власника процесу/інформації
- Як визначаються та пом’якшуються ризики інформаційної безпеки (шляхом застосування засобів контролю, що відповідають рівню ризику, юридичним вимогам і вимогам відповідності та класифікації інформації)

2) Політика безпеки
    - Офіційна документація принципів, якими компанія керує своєю програмою інформаційної безпеки (наприклад, політика програми інформаційної безпеки)
    - Переглядається та зберігається поточна політика, стандарти та процедури щодо інформаційної безпеки та інформаційних технологій, включаючи офіційний огляд та затвердження керівництва (принаймні раз на рік)
    - Призначений розпорядник вашої програми інформаційної безпеки, а також політик і процесів, які її підтримують
    - Обізнаність з застосовними політиками, стандартами та процесами інформаційної безпеки
    - Офіційна документація принципів, які керують тим, як компанія захищаєте свою інформацію (наприклад, політика захисту інформації)
3) Фізична та екологічна безпека

- Виробничі приміщення мають контроль температури, вологості, якості повітря, запобігання пожежі та диму, виявлення та гасіння, електростабільність, захист від пошкодження водою.
- Яким чином вимикачі живлення захищені від випадкового або несанкціонованого відключення
- Офіційна документація про наявні засоби контролю для ефективного управління фізичною безпекою / доступом до ваших об'єктів
- Відеоспостереження за всіма комп’ютерними залами та всіма входами по периметру існує і чи вирівняно воно, щоб чітко бачити обличчя людей із прийнятною якістю відео
- Чи не публічні заклади повинні мати фізичний контроль доступу, який обмежує доступ уповноваженим особам; Повинна бути реєстрація доступу для співробітників, підрядників і відвідувачів
- Системи виявлення зловмисників і сигналізації (наприклад, примусове відкриття дверей, відкриті двері, несправний пристрій); Аварійні виходи тривожні цілодобово
- Співробітники, підрядники та відвідувачі повинні носити посвідчення особи, яке завжди видно
- Робочі станції та пристрої, що використовуються для зберігання, обробки або передачі будь-яких конфіденційних даних, повинні бути заблоковані або вимкнені, якщо їх немає.

4) Безпека мережі та програмного забезпечення
    - Процедури посилення мережі, використання Інтернету, захисту бездротових мереж
    - Політика та процедури адміністрування облікових записів користувачів для всіх підтримуваних платформ, де обробляються цільові дані та пов’язаний доступ до мережі
    - Реєстрація мережевої активності

- Схеми конфігурації мережі та стандарти для внутрішніх і зовнішніх мереж визначені в області застосування
- Політики та процедури щодо таких сфер управління змінами:
- Документація для впровадження та результати випробувань
- Політики та процедури щодо розкладу резервного копіювання, ротації, за межами сайту

5) Управління доступом
    - Контроль доступу до програм, систем, баз даних, мереж і віддаленого доступу
    - Політики та процедури щодо запиту та надання доступу користувачам (включаючи анулювання/вилучення доступу)
    - Управління даними та стандарти класифікації
    - Використання та стандарти шифрування
    - Процедура виявлення невдалих спроб входу
    - Можливості віддаленого входу, особливо «дистанційна робота»
    - Вимоги до ідентифікатора користувача та пароля для доступу до мобільних пристроїв, конфіденційної документації, електронної пошти та інших технологій
    - Супровідна документація, що свідчить про завершення періодичних перевірок прав користувача
6) Безпека людських ресурсів
    - Співробітники, підрядники та треті сторони навчаються щодо їхніх обов'язків щодо безпеки та захисту інформаційних ресурсів
    - Навчання з питань безпеки проводиться щорічно протягом 30 днів після прийняття на роботу
    - Проводиться перевірка даних
7) Управління змінами
    - Офіційні процеси управління змінами (включаючи поділ обов'язків для тих, хто запитує, затверджує та впроваджує зміни)

- Документовані процеси побудови та підтримки інформаційних систем (наприклад, політика операцій з інформаційної безпеки)
- Документований процес або процедура сканування уразливостей безпеки програми
- Регулярний статичний аналіз коду, оцінка вразливостей та обсяг і частота тестів на проникнення
- Програмне забезпечення та програми, що використовуються для підтримки бізнесу American Express Global Business Travel, дотримуються встановлених процесів:

- Належним чином авторизовані, придбані або створені за допомогою процесів, які включають критерії безпеки та оцінку
- Розроблено та реалізовано відповідно до вимог безпеки
- Налаштований для своєчасного усунення відомих вразливостей і загроз
- Періодично переоцінюється, щоб усунути зміни в ландшафті вразливості

8) Безперервність обслуговування

- Офіційна документація для керування безперервністю обслуговування за допомогою встановлених планів безперервності бізнесу та аварійного відновлення (наприклад, політика безперервності обслуговування)
- Плани безперервності бізнесу та аварійного відновлення розповсюджуються всім, хто бере участь у відновленні процесу/послуги/функції, а результати вправ публікуються для відповідних осіб та керівництва.

9) Управління активами

- Документований процес або процедура виявлення конфіденційної інформації

- Для захисту конфіденційної інформації від неналежного розкриття, неправильного використання та несанкціонованого доступу, відповідно до її класифікації, існують документовані засоби контролю
- Чи має компанія офіційну документацію, яка визначає засоби контролю для ефективного керування обробкою та утилізацією інформації
- Опис процесів передачі інформації та керування ними
- Застосовані засоби контролю, які гарантують, що ваші системи та/або процеси забороняють використання знімних носіїв
- Офіційна документація принципів, які керують тим, як ви класифікуєте інформацію (наприклад, політика класифікації інформаційної безпеки)
- Конфіденційна інформація має призначеного зберігача з визначеними обов'язками

Раз на 5 років компанія American Express Global Business Travel проводить аудит своїх партнерів на відповідність стандартам інформаційної безпеки. Дана перевірка проводиться у вигляді листа опитування, де на кожен пункт компанія має дати відповідь та роз'яснення у разі не відповідності стандарту. Після проведення даного опитування компанія отримує рекомендації по усуненню недоліків та зобов'язується усунути їх протягом відведеного на це часу. Його кількість American Express Global Business Travel для кожного партнера визначає в індивідуальному порядку, в залежності від об'ємів необхідних робіт.

Таблиця 3.1 відповідає листу опитуванню, що був мною розроблений для ПрАТ «Обрій Інк.» [Додаток А, розроблений автором мовою оригіналу], щоб забезпечити проходження аудиту відповідності програмі інформаційної безпеки від міжнародного партнера, також в ній зазначені актуальні відповіді, які були виявлені шляхом проведення внутрішнього аудиту.

Запитання були сформульовані опираючись на вимоги American Express Global Business Travel у відношенні інформаційної безпеки бізнесу.

№	Запитання	Відповідь
1	Чи є у вашій компанії власники процесів та інформації, які визначають, оцінюють, пом'якшують інформаційні ризики та керують ними? (Власники процесів і інформації несуть відповідальність за ризики інформаційної безпеки, пов'язані з бізнес-процесами, підтримкою технологічних рішень, іншими інформаційними ресурсами)	Так
2	Чи існує у вашій компанії офіційний документований процес оцінки ризиків інформаційної безпеки, який включає нагляд власника процесу/інформації?	Ні
3	Чи є у вашій компанії офіційна документація з принципами, якими ви керуєте своєю програмою інформаційної безпеки?	Так
4	Чи перевіряє ваша компанія свою політику, стандарти та процедури щодо інформаційної безпеки та інформаційних технологій, включаючи офіційну перевірку та затвердження керівництва?	Так
5	Чи є у вас призначений розпорядник вашої програми інформаційної безпеки, а також політик і процесів, які її підтримують?	Так
6	Чи має ваша компанія офіційну документацію про принципи, які керують тим, як ви керуєте поінформованістю всіх найнятих осіб	Так

	(співробітників, підрядників і третіх сторін) про застосовні політики, стандарти та процеси інформаційної безпеки?	
7	Чи має ваша компанія офіційну документацію з принципами, які керують тим, як ви захищаєте свою інформацію?	Ні
8	Чи застосовуються заходи в приміщеннях, які забезпечують належний контроль температури, вологості та якості повітря?	Так
9	Чи застосовуються заходи на об'єктах, які забезпечують належне запобігання, виявлення та гасіння пожежі та задимлення?	Так
10	Чи використовуються заходи об'єктах, які забезпечують захист від пошкодження водою (включаючи конденсацію, яка може пошкодити електричні схеми)?	Так
11	Чи існують відповідні засоби захисту для вимикачів живлення?	Так
12	Чи має ваша компанія офіційну документацію, яка визначає засоби контролю для ефективного управління фізичною безпекою/доступом до ваших об’єктів?	Так
13	Чи регулярно переглядається список осіб, які мають фізичний доступ до конфіденційних областей, де зберігаються, передаються або обробляються дані GBT та/або коли відбуваються зміни в персоналі?	Так
14	Чи існує відеоспостереження за всіма комп’ютерними залами та всіма входами по периметру, і чи вирівняно воно, щоб чітко бачити	Так

	обличчя людей із прийнятною якістю відео?	
15	Чи є у непублічних приміщеннях засоби контролю фізичного доступу, які обмежують доступ уповноваженим особам?	Так
16	Чи мають негромадські об’єкти засоби контролю фізичного доступу, які реєструють особистість, час прибуття та від’їзду всіх осіб (тобто працівників, підрядників та відвідувачів)?	Так
17	Чи є негромадські об’єкти належним чином захищеними, з можливостями виявлення зловмисників, які відповідають національним, регіональним або міжнародним стандартам?	Так
18	Чи є в негромадських приміщеннях аварійні виходи, які цілодобово доступні?	Так
19	Чи всі відвідувачі попередньо схвалені, і чи мають вони надати діючі державні документи, перш ніж отримати доступ до об’єктів внутрішнього використання?	Ні
20	Чи зобов’язані працівники, підрядники та відвідувачі носити посвідчення, яке завжди видно?	Ні
21	Чи розрізняють посвідчення між працівниками, підрядниками та відвідувачами?	Так
22	Чи має ваша компанія офіційну документацію з принципами, якими ви керуєте фізичною та екологічною безпекою своїх об’єктів? (наприклад, політика безпеки об'єктів)	Так
23	Чи робочі станції та пристрої, які використовуються для зберігання, обробки або передачі будь-яких конфіденційних даних, блокуються або вимикаються,	Так

	а також фізично захищені, коли вони не використовуються?	
24	Чи контролюєте ви бездротовий доступ до своїх інформаційних систем?	Так
25	Чи має ваша компанія офіційну політику, яка забороняє встановлення несанкціонованого апаратного чи програмного забезпечення?	Так
26	Чи є у вашій компанії офіційний, задокументований процес або процедура, яка забезпечує резервне копіювання та відновлення інформації?	Так
27	Чи створено резервну копію критичної для бізнесу інформації та чи можна її відновити у разі збоїв устаткування, пошкодження даних, стихійного лиха чи будь-якого іншого інциденту, який може знищити вихідні дані?	Так
28	Чи має ваша компанія офіційну документацію, яка визначає засоби контролю для ефективного захисту інформаційних ресурсів від шкідливого коду?	Так
29	Чи встановлено у вас засоби безпеки, які захищають ваші інформаційні ресурси (настільні комп’ютери, ноутбуки та сервери) від зловмисної діяльності? (Засоби безпеки повинні виявляти, запобігати, видаляти та відновлювати зловмисну діяльність, яка здійснюється проти ваших настільних комп’ютерів, ноутбуків і серверів)	Так
30	Чи відповідають встановлені вами засоби безпеки наступним критеріям? • Налаштований на запуск під час запуску та безперервний запуск	Так

	• Налаштовано на виявлення та захист від шкідливих дій • Підтримується та періодично перевіряється на наявність оновлень • Керується тими, хто має відповідні повноваження та дозволи (Засоби безпеки повинні виявляти, запобігати, видаляти та відновлювати зловмисну діяльність, яка здійснюється проти ваших настільних комп'ютерів, ноутбуків і серверів)	
31	Чи використовуються брандмауери під час підключення вашої надійної мережі до ненадійної мережі?	Ні
32	Чи періодично перевіряються та оновлюються правила брандмауера, щоб гарантувати, що встановлені лише коректні правила?	Так
33	Чи має компанія офіційну документацію, яка визначає, як ви відстежуєте та керуєте мережевим трафіком?	Ні
34	Чи відстежується, контролюється, керується та періодично оцінюється мережевий трафік для виявлення вразливостей?	Ні
35	Чи надають засоби керування брандмауером лише затвердженим пристроям доступ до внутрішньої мережі?	Так
36	Чи виконуєте ви сканування мережі/сервера та тести на проникнення, використовуючи надійні продукти, щоб виявити прогалини в безпеці?	Ні
37	Чи є у вас задокументовані процеси для відстеження	Ні

	та обліку мережевих пристроїв, щоб гарантувати, що лише легальні, ліцензовані та затверджені IT-активи розгортаються в середовищі протягом усього їхнього життєвого циклу?	
38	Чи ваша мережа сегментована між географічними регіонами, бізнес-підрозділами або важливими активами для захисту конфіденційної інформації?	Ні
39	Чи весь доступ кінцевих користувачів до Інтернету здійснюється через проксі-сервер користувача?	Ні
40	Чи відокремлені ваші сегменти бездротової мережі від внутрішніх мереж за допомогою віртуальної локальної мережі або інших відповідних технологій?	Так
41	Чи обмежено прямий мережевий доступ до виробничих і невиробничих серверів?	Так
42	Чи має компанія офіційну документацію, яка визначає засоби контролю для ефективного керування віддаленим доступом до інформаційних систем?	Так
43	Чи використовуються рішення для багатофакторної аутентифікації?	Так
44	Чи має компанія офіційну документацію, яка визначає засоби контролю для ефективного управління розподілом обов’язків?	Так
45	Чи включають процеси та засоби контролю принцип «розподілу обов’язків» для захисту критичних інформаційних ресурсів?	Так
46	Чи застосовується принцип розподілу обов’язків для контролю доступу до виробничої інформації?	Так
47	Чи має компанія офіційну документацію, яка	Так

	визначає засоби контролю для ефективного керування виправленнями та оновленнями програмного забезпечення?	
48	Чи перевіряються виправлення програмного забезпечення на предмет застосовності та чи впроваджуються належним чином з тестуванням перед встановленням?	Ні
49	Чи отримуються виправлення програмного забезпечення через регулярний, встановлений, автоматизований процес?	Так
50	Чи має компанія офіційну документацію, яка визначає засоби керування для ефективного керування конфігураціями операційних систем і технологічних продуктів у внутрішньому середовищі?	Так
51	Ваші системи та програми захищені від неправомірного використання, несанкціонованого розкриття та пошкодження?	Так
52	Чи є засоби контролю, які гарантують, що дані, які використовуються для тестування, ніколи не будуть переміщені або скопійовані у виробниче середовище?	Так
53	Чи є у компанії офіційна документація, яка визначає, як керується доступом до інформації (тобто засоби контролю доступу)?	Так
54	Чи визначено правила чи принципи для призначення доступу до інформаційних систем?	Так
55	Чи існують засоби контролю, які забезпечують схвалення або дозвіл доступу до інформації	Так

	власником інформаційного ресурсу?	
56	Чи існують засоби контролю, які забезпечують видалення доступу до інформації, коли вона більше не потрібна?	Так
57	Чи має компанія офіційну, задокументовану політику, процес або процедуру, яка забезпечує надійний захист облікових даних автентифікації (наприклад, паролі, парольні фрази, таємні запитання/відповіді, PIN-коди)?	Так
58	Чи є засоби контролю, які гарантують, що системи або процеси не підтримують надання копії пароля через Інтернет за допомогою незахищеної електронної пошти?	Ні
59	Чи існують механізми для блокування інтерфейсу користувача пристрою після певного періоду бездіяльності?	Ні
60	Чи є у вашій компанії офіційна документація, яка визначає засоби контролю для ефективного керування блокуванням інтерфейсів користувача?	Ні
61	Чи потрібна повторна аутентифікація під час відновлення доступу до інтерфейсу пристрою?	Так
62	Чи створюється, зберігається та керується інформація з використанням лише затверджених систем, обладнання та програмного забезпечення з засобами контролю, які забезпечують використання такої інформації лише для бізнес-цілей?	Так
63	Чи навчаються співробітники, підрядники та треті сторони щодо їх відповідальності щодо захисту та захисту інформаційних ресурсів?	Так

64	Чи беруть участь особи щорічно в тренінгах з інформаційної безпеки та підтверджують їх перевірку протягом 30 днів після прийняття на роботу?	Так
65	Чи має компанія офіційну документацію, яка визначає засоби контролю для ефективного управління змінами?	Так
66	Чи має компанія офіційну документацію про принципи, які керують тим, як будуються та підтримуються інформаційні системи відповідно до документованих конфігурацій і стандартів?	Так
67	Чи має компанія офіційну документацію з принципами, які керують тим, як ви керуєте інцидентами інформаційної безпеки?	Так
68	Чи є засоби контролю, які гарантують, що ваші системи та/або процеси забороняють використання знімних носіїв?	Так
69	Чи має компанія офіційну документацію з принципами, які керують тим, як класифікується інформація?	Так
70	Чи є у компанії офіційна документація, яка детально описує вимоги щодо забезпечення всієї конфіденційної інформації призначеного зберігача з визначеними обов’язками?	Так

Таблиця 3.1 Лист опитування. Джерело: розроблено автором

При обстеженні інформаційних систем були проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації,

архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

- види і характеристики каналів зв'язку;
- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного.

Були виявлені компоненти інформаційних систем, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів інформаційних систем, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

На основі проведеного дослідження були розроблені рекомендації для ПрАТ «Обрій Інк.» щодо усунення виявлених недоліків.

3.2. Рекомендації, щодо усунення виявлених недоліків

Система управління інформаційною безпекою ПрАТ «Обрій Інк.» є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка побудована на кращих світових практиках. Проте, під час проведення аудиту системи інформаційної безпеки, були виявлені деякі недоліки, для усунення яких були складені методичні рекомендації.

1) Методичні рекомендації щодо управління ризиками інформаційної безпеки розроблені на основі міжнародного стандарту ISO/IEC 27005 "Information technology - Security techniques - Information security risk management" (Управління ризиками інформаційної безпеки – Додаток Б). Управління інформаційними ризиками повинно включати:

- аналіз і ідентифікацію ризиків;

- оцінку ризиків з точки зору їх впливу на бізнес та ймовірності їх появи;
- інформування особи, яка вправі приймати рішення та акціонерів компанії про ймовірності та впливи цих ризиків, ймовірність і наслідки ризику мають бути зрозумілими;
- встановлення порядку та пріоритетів оброблення ризиків;
- встановлення пріоритетів виконання дій щодо зниження
- ризиків;
- участь керівництва в процесі прийняття рішень щодо
- управління ризиками та його поінформованість щодо стану справ в
- управлінні ризиками;
- ефективний моніторинг та регулярний перегляд ризиків і
- процесу управління ризиками;
- інформування керівництва та персоналу щодо ризиків і дій
- щодо управління ними.

Процес управління ризиками інформаційної безпеки стосується всіх підрозділів компанії і, у першу чергу, керівників підрозділів - власників бізнес-процесів / продуктів. Тому ці відповідальні особи повинні брати участь у вирішенні питань, що належать до сфери їх відповідальності.

2) Всі активи компанії мають бути оцінені за наступними критеріями, що допоможе визначити ризики втрати інформації:
    - конфіденційність - властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;
    - цілісність - властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. Цілісність системи - властивість системи, яка полягає в тому, що жоден її компонент

не може бути усунений, модифікований або доданий з порушенням політики безпеки;

- доступність - властивість ресурсу системи, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;
- спостережність - властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Для різних бізнес-процесів / продуктів можуть бути виявлені однакові ризики втрати основних сервісів безпеки, що буде свідчити про те, що певним питанням інформаційної безпеки не приділяється необхідної уваги. У такому випадку рекомендується вирішувати питання зменшення ризиків однаково для всіх бізнес-процесів / продуктів компанії.

3) Для виявлення вразливостей, в залежності від критичності інформації та бізнес-процесу / продукту, а також від інформаційних технологій можуть використовуватися різні проактивні методи тестування. Такі методи тестування включають:
    - спеціальний автоматичний інструментарій для сканування вразливостей;
    - тестування та оцінку безпеки;
    - тести на проникнення;
    - перегляд коду програмно-технічних комплексів;

- аналіз відомих порушень безпеки;
- аналіз відомих вразливостей (наприклад, операційних систем, баз даних, технологій та протоколів тощо).

Такі методи допоможуть ідентифікувати вразливості. Слід зазначити, що іноді ці методи можуть надавати інформацію про вразливості, які не представляють реальної загрози. Тому необхідно чітко задавати параметри програмно-технічних комплексів та їх конфігурацію для тестування.

4) Найуразливішою стороною системи інформаційної безпеки є людський ресурс (працівники компанії). Для забезпечення безпеки людських ресурсів необхідні:
    - Процедури управління персоналом;
    - Критерії прийому персоналу;
    - Опис процедури перевірки кандидатів на прийом на роботу
    - Опис процедури навчання прийнятих на роботу працівників вимогам щодо інформаційної безпеки;
    - Опис процедури підготовки посадових інструкцій;
    - Опис дисциплінарного процесу щодо персоналу, який здійснив порушення безпеки;
    - Опис процедури звільнення персоналу з точки зору припинення відповідальності, скасування прав доступу та повернення ресурсів компанії;
    - Програма навчання персоналу.

Особливу увагу слід звернути на людські джерела загроз, які можуть мати різну мотивацію від комерційних причин до простого самоствердження. Найбільш вірогідними та найбільш серйозними можна вважати загрози від власних працівників банку, в тому числі ті загрози, які можуть виникати від недостатньої обізнаності персоналу в питаннях інформаційної безпеки.

ВИСНОВКИ

Поняття загрози інформаційної безпеки зародилось майже у той же час, як і поява інформаційного середовища. Спочатку це були прояви крадіжки інформації з комп'ютера, незаконне використання, порча інформації на комп'ютерах. Пізніше з розвитком інформаційних мереж інформаційна небезпека перетворилась в засоби перекачування по мережі неправдивої інформації, вірусів. Зараз питання безпеки відноситься майже до всіх агентів глобального інформаційного середовища. Україна як активний учасник процесів циклу життя інформації не стоїть в стороні від них. Це відбувається як на загальному міжкраїновому рівні, так і в середині кожного окремого підприємства.

На сьогоднішній день нагальною постає проблема збільшення інформаційної безпеки підприємства, яка значною мірою залежить від ступеня захищеності інформаційної сфери. Рівень інформаційної безпеки впливає на розвиток та впровадження науково-технічних інновацій у процеси виробництва, збереження стабільності функціонування можливості економічного зростання.

Розвиток бізнесу перебуває у постійному русі і динамічно змінюється під впливом конкуренції та процесів глобалізації. Глобальний етап інтеграції економічних систем безпосередньо пов'язаний з багатоплановим процесом розширення та поглиблення світогосподарських зв'язків завдяки підвищенню мобільності факторів і результатів виробництва (макрорівень) та залучення фірми до міжнародних операцій (мікрорівень). Під впливом глобальних процесів спостерігається прискорення науково-технічного прогресу, розширюється обмін новими, зокрема, збільшується кількість здійснення фінансових видів послуг. Проте під швидкими темпами зростання економічних процесів при здійсненні господарської діяльності зростає і роль інформаційної безпеки підприємства. При веденні своєї діяльності підприємець обов'язково наштовхується на необхідність отримання,

обробки, зберігання, перетворення, передачі та ліквідації непотрібної інформації. Якщо деяка інформація є цінною для підприємця, то її треба охороняти від зловмисників. Цінність визначається через ряд параметрів, до яких належать корисність, достовірність, своєчасність, релевантність. При захисті інформації слід перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на усіх носіях, що маються на підприємстві. Загрози інформаційної безпеки поділяються на внутрішні та зовнішні.

Зовнішні зловмисні дії можуть бути такими:

– копіюванні цінних документів, або викрадення файлів;

– викрадення флеш-карт;

– викрадення інформації у процесі її передавання по мережі Інтернет;

– пошкодження носіїв з інформацією;

– донесення інформації до фірм-конкурентів, або взагалі до іншої країни;

– викрадення інформації за допомогою інсайдерів;

– переманювання персоналу на іншу фірму.

До найбільш поширених внутрішніх загроз відносяться крадіжка, зараження

інформації вірусами, або порча файлів службовцями компанії. До причин внутрішніх загроз відносяться:

– причини психологічного характеру у зв’язку з відносинами між співробітниками підприємства, що не склалися;

– незадоволення рівнем заробітної плати;

– недобрі відносини між співробітником та керівництвом компанії;

Психологи стверджують, що біля 25 % всіх співробітників підприємств розголошують інформацію, продають або передають її конкуруючим компаніям задля додаткового заробітку.

Захист інформації на підприємстві є дуже важливою річчю і цей аспект повинен бути обов'язковим при укладанні контракту компанією з її працівником, особливо якщо цей працівник займає керуючу посаду в компанії.

Небезпека, в першу чергу, загрожує інформації, яка зберігається в інформаційних системах підприємства. У цю систему входять програмне забезпечення автоматизованої системи, програми для виконання конкретних задач компанії, програмні оболонки, текстові редактори, пакети програм, бази даних. Інформація може поступати по локальній мережі з пристрою введення, а саме з клавіатури, з зовнішнього середовища, а саме з мережі Інтернет, від інших компаній.

Щоб гарантувати безпеку інформаційної системи підприємства, необхідним є наділення повноважень зареєстрованим користувачам, серед яких можутьбути як певні особи, так і організації. Ці користувачі можуть здійснювати тільки визначені наперед дії з використанням інформаційних технологій.

Підчас проведення дослідження заходів інформаційної безпеки на ПрАТ «Обрій Інк.» за основу і стандарти була взята програма з захисту інформації міжнародного партнера – American Express Global Business Travel.

На основі міжнародних вимог був складений лист-опитування, за допомогою якого вдалося проаналізувати чи відповідає ПрАТ «Обрій Інк.» вимогам свого глобального партнера. Під час дослідження були виявлені певні недоліки, для усунення яких були складені методичні рекомендації і переданіменеджменту компанії для розгляду та впровадження.

На мою думку, компанія дуже відповідально ставиться до питань інформаційної безпеки, має більшість необхідних документів для фіксації та визначення норм та правил інформаційної безпеки, що дає змогу чітко визначити будь-які неправомірні дії у відношенні активів компанії згідно з їх класифікацією та необхідним рівнем захисту. У компанії чітко розподілені активи між їх власниками або відповідальними особами та складений нормативний документ щодо керування активами та надання доступів різного рівня.

РЕЗЮМЕ

Кваліфікаційна робота на тему «Інформаційна безпека бізнесу сучасної організації» виконана на базі практики ПрАТ «Обрій Інк.».

Метою кваліфікаційної роботи магістра є розробка шляхів вдосконалення інформаційної безпеки на ПрАТ «Обрій Інк.» теоретичних основ та сутності методів вдосконалення систем інформаційної безпеки, систематизація, закріплення та поглиблення знань набутих у процесі навчання та їхпрактичної реалізації, що полягають у розробці рекомендацій щодо вдосконалення систем інформаційної безпеки на ПрАТ «Обрій Інк.».

У першому розділі кваліфікаційної роботи було визначено сутність поняття інформаційної безпеки, досліджені принципи використання концепцій та правил інформаційної безпеки в системі управління підприємством, структуру служби інформаційної безпеки організації та принципи захисту віддаленого доступу до мережі компанії.

У другому розділі було надано загальну характеристику ПрАТ «Обрій Інк.», визначено особливості організаційної структури ПрАТ «Обрій Інк.» та проаналізовано економічні показники діяльності чинного підприємства.

У третьому розділі надані рекомендацій щодо вдосконалення систем інформаційної безпеки на актуальність теми дослідження.

Одержані результати, що мають прикладний характер, використані на практиці підприємства ПрАТ «Обрій Інк.».

Рік виконання дипломної роботи – 2021.

Рік захисту роботи – 2021.

RESUME

Qualification work on the topic "Information security of business of modern organization" was performed on the basis of the practice of JSC OBRIY INC.

The purpose of the master's qualification work is to develop ways to improve information security at JSC OBRIY INC. theoretical bases and essence of methods for improving information security systems, systematize, consolidate and deepen the knowledge acquired in the course of training and their practical implementation, which are to develop recommendations information security at JSC OBRIY INC.

In the first section of the qualification work the essence of the concept of information security was defined, the principles of using concepts and rules of information security in the enterprise management system, the structure of the information security service of the organization and the principles of remote access to the company's network.

In the second section, the general characteristics of JSC OBRIY INC. were presented, the features of the organizational structure of JSC OBRIY INC. were determined, and the economic indicators of the activity of the current enterprise were analyzed.

The third section provides recommendations for improving information security systems for the relevance of the research topic.

The obtained results, which are applied in nature, were used in the practice of the company JSC OBRIY INC.

Year of completion of the thesis - 2021. Year of protection of work - 2021.

Характеристика джерела	**СПИСОК ВИКОРИСТАИХ ДЖЕРЕЛ**
Один автор	1. Абакумов В.М. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони / В.М. Абакумов // Форум права. – 2012. – № 4. – С. 10-16. 2. Верескун М.В. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М.В. Верескун // Економіка і організація управління. – 2014. – № 1 (17). – С. 54-60. 3. Ганієв А. Капітал акціонерного товариства: принципи формування, оптимізація структури// Ринок цінних паперів України. – 2002. – № 7/8. – С. 41-45. 4. Гуцалюк М. Інформаційна безпека України: нові загрози // Бизнес и безопасность. - 2003. - № 5. - С. 2-3 5. Замкова Т.В. Проблемы защиты информации в современных информационных системах / Т.В. Замкова. – [Електронний ресурс]. – Режим доступу: http://www.rae.ru/snt/?section=content&op=show_article&article_id=3 893 6. Захаров Е. Информационная безопасность или опасность отставания?// Права людини. - 2000. - № 1 . - С. 3-5 7. Зубок М.І. Інформаційне забезпечення підприємницької діяльності // Інформаційна безпека в підприємницькій діяльності – 2014. – С. 143-145 8. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами // Альманах економічної безпеки. - 1999. - № 2. - С. 15-17 9. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич,. -К.: Кондор, 2005. -382 с. 10. Легомінова С.В. Теоретичні засади інформаційної безпеки підприємства / С.В. Легомінова // Економіка. Менеджмент. Бізнес. – 2015. – № 3 (13). – С. 87-92.

	11. Романова Ю.Д. ІНФОРМАЦІЙНА БЕЗПЕКА БІЗНЕСУ // Інформаційні технології в менеджменті (управлінні) – 2015 12. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ // Актуальні проблеми економіки. - 2006. - № 10. - С. 220 - 225.
Два автори	1. Басовский Л.Е., Протасьев В.Б. Управление качеством. М. : ИнфраМ., 2002. 2. Белошапка В.А. Управленческая результативность: системный подход на работу и развитие менеджеров: учеб. [для практикующих менеджеров] / В.А. Белошапка, И. В. Нудьга. К.: Агентство "Стандарт", 2007. 270 с.
Чотири і більше авторів	1. Батюк А.Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – [С. 343–384.].
Колективнийавтор	1. Менеджмент організацій: Підручник. Колектив авторів за заг. ред. Л.І.Федулової. К.: Либідь, 2004. 448 с.
Статті з продовжуючихта періодичнихвидань	1. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть // Вісник Київського університету імені Т.Шевченка. - 1999. - Вип. 14: Міжнародні відносини. - С. 46-48 2. Кучеренко Т. Є. Теоретичне обґрунтування фінансових результатів в контексті моделі балансу / Т. С. Кучеренко // Вісник ХНАУ. Серія "Економіка АПК і природокористування". – 2009. – № 13. – С. 230-237.

Законодавчі та нормативні документи	1. Господарський кодекс України: Кодекс України від 16.01.2003 №436- IV / Верховна Рада України. – К.: Юрінком Інтер, 2006. 304 с. 2. Закон України «Про зовнішньоекономічну діяльність» від 16.04.91р. №959-XII із змінами і доповненнями. / Вісник Верховної Ради України. – 2012. – №7. 3. Закон України Про порядок здійснення розрахунків в іноземній валюті . (2019) URL: https://zakon.rada.gov.ua/laws/show/185/94-%D0%B2%D1%80 (дата звернення: 19.10.2021). 4. Закон України «Про охорону прав на комерційну таємницю» - [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1404-2008-%D1%80 5. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: від 09.01.2007 р., № 537. 6. Конституція України: Закон Верховної Ради України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996. №30. Ст. 141. 7. Митний кодекс України . (2019) URL: https://zakon.rada.gov.ua/laws/show/4495-17 (дата звернення: 19.10.2021). 8. Система забезпечення інформаційної безпеки України // Національна безпека і оборона. - 2001. - № 1. - С. 16-28
Стандарти	1. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

ДОДАТКИ

Додаток А

Таблиця 3.1 Лист опитування (мовою оригіналу)

Information Security Risk Management	**Answer**	**Comments**
Does your company have process owners and information owners who identify, assess, mitigate and manage information risks? (Process owners and information owners are responsible for information security risks associated with • business processes • supporting technology solutions, and • other information resources)	**YES**	
Does your company have a formal, documented information security risk assessment process which incorporates process/information owner oversight?	**NO**	We have information security management plan document, which covers roles and responsibilities, incident management, vulterability management and threat management etc..
Security Policy		

Does your company review and keep current its information security and information technology policies, standards and procedures, incorporating formal leadership reviewand approval? if N/A: Elaborate why this is not applicable.	**YES**	Every policy/standard/procedure has its owner who may alsoengage with other stakeholders todevelop the policy, after the policy is developed and agreed with all parties in the scope it is approved by General Director. All policies approved by General Director are distributed/published to all staff (shared drive + e-mail communication with the path). The line managers are required to make sure employees have reviewed and adhere
Do you have a designated custodian for your information security program and for the policies and processes that support it?	**YES**	Svitlana Styopochkina - IT Director. Svitlana is overlooking all third party relationships with IT vendors (including hardware, software, SAAS), overlooking all internal data infrastructure and hardware infrastructure. Therefore she is competent to establish policies and procedures for information security.
Does your company have formal documentation of principles that guide how you protect your information?(e.g., an	**NO**	it is mandatory that there are personal NDAs with employeesin place before they start workingon company assignments (this requirement also works for

Information Protection policy)(Information must be securely managed and protected based upon its information security classification.)		contractors) and general Information security policy awareness training (Induction) + Information security training (annual refresher) are mandatory as well
Physical and Environmental Security		
Are information resources used for production processing located in facilities that ensure appropriate temperature, humidity and air-quality controls?	**YES**	yes, in the server-room there are two air conditioners and the appropriate termperature and humidity is ensured (themeasures are taken)
Are information resources used for production processing located in facilities that ensure appropriate fire and smoke prevention, detection and suppression?	**YES**	there is no automatic fire suppression, the manual fire extinguisher is available. There is automatic detection (fire and smoke/high temperature), once the incident is detected - the emergency signal goes directly to the central fire station of the security policy of Kyiv city + alarm in the facility to prompt evacuation
Are information resources used for production processing located in	**YES**	there are two UPS (uninterruptible power sources) providing power supply in

facilities that ensure electrical power stability?		emergency situations for short terms incidents, for longer term - there are 2 independent sourcesof input power therefore if one is off for emergency reasons - we switch to another one while in UPS mode. and vice versa.
Are information resources used for production processing located in facilities that ensure protection from water damage (including condensation which can damage electrical circuitry)?	**YES**	in server room there is a condensation removal system including dreinage pump which removes the condesate directly into central severage system
Are there appropriate safeguards for power switches? (Intent is to prevent accidental or unauthorized powering off of critical equipment.)	**YES**	there are two UPS (uninterruptible power sources) providing power supply in emergency situations for short terms incidents, for longer term - there are 2 independent sourcesof input power therefore if one is off for emergency reasons - we switch to another one while in UPS mode. and vice versa.
Does your company have formal documentation that identifies the controls in place to effectively manage	**YES**	there is automated gating system for office in/out and critical premises in/out with badges giving access only to limited

physical security / access at your facilities?		areas as per the employee roles. + there are lists for the premises opening/closing authorizations (overnigh opening/closure)
Is the list of persons with physical access to sensitive areas where GBT data is stored, transmitted, or processed, reviewed regularly and/or when there are changes to personnel?	**YES**	very limited headcount to worry about the visibility of badges. We know everyone personally. Still badge is required to get in/out.
Does video surveillance ofall computer rooms and all perimeter entrances existand is it aligned to clearly see people's faces with acceptable video quality?	**YES**	yes, all entrances/exists have surveillance, all operational rooms, the server room does not have surveillance inside but the entrance is visible from one ofthe cameras. The quality is good to see the faces.
Do non-public facilities have physical access controls that limit access to authorized individuals? (This includes access into the facility as well as into areas within the facility that are of heightened security concern (e.g., computer centers, cable and wiring closets, etc.).)	**YES**	gating system

Do non-public facilities have physical access controls that log the identity, time of arrival and departure of all individuals (i.e., employees, contractors and visitors)?	**YES**	Gating system + phisical log record for overnight closure/opening. For visitors - phisical log record
Are non-public facilities suitably alarmed, with intruder detection capabilities that meet national, regional or international standards?	**YES**	The glass-break detectors are present on all windows, in all premises - motion detectors. In case of eny incident - alarm is triggered and the security policy gets the signal and sends the squad, also the HSE custodian is notified immediately.
Do non-public facilities have emergency exits that are alarmed on a 24x7 basis?	**YES**	it`s not alarmed by any lighting/illumination but is clearly marked with "emergency exit" signage. There are two emergency exists in addition to the central exit.
Are all visitors pre-approved, and must they provide current government issued identification before being granted access to non-public facilities?	**NO**	always pre-approved, no need for government issued ID as we normally know the invitees. They are always accompanied by company employee (the host)

Are employees, contractors, and visitors required to wear an identification badge that is visible at all times?	**NO**	Employees - YES, but even if they don`t wear it is not criticalas we are relatively small company. For GUESTs (see below), for permanent contractors (same as employees). Due to gating system - no strangers expected. Still, a security guard or any representative of company management is entitled to check the person`s identity if the individual is not known and not accompanied by the known staff member.
Do identification badges distinguish between employees, contractors and visitors?	**YES**	the "GUEST" badge is available for visitors. Alternatively (as number of such badges is limited) - the visitors might be acceptable without badges if accompanied by an employee at all times.
Does your company have formal documentation of principles that guide how you manage the physical and environmental security of your facilities? (e.g., a Facilities Security policy) (Third parties shall adhere to	**YES**	There is no one policy but there are different instrucation and procedures. Owner - HSE responsible Volodymyr Bobyr. There is the job description of security guard, the instruction on opening/closures of the facility premises overnight, the lists of authorizes individuals, the

the same informationsecurity policies and standards you have established with GBT.)		evacuation plans, fire alarming plans etc....
Are workstations anddevices used to store, process or transmit any sensitive data locked or logged off when unattended, and physically secured whennot in use?	**NO**	might be locked in a separate non-operational room/storage when not in use. This is not mandated however But even if the PC is waiting for its next user in the work environment - as there are no public accessible areas and there is access control (gating system) and video survillance - we see it compensated
Network and Software Security		
Do you control wireless access to your information systems?	**YES**	the wireless connection to our network requires two factor authentication which includes the certificate preliminary issued/installed on a equipment + login and password. This access is only provided to employees who require such access per their role. The guest wi-fi does not require certificate and does not provide access to our network, internet connection only (for

		guests/visitors)
Does your company have a formal policy whichprohibits the installation of unauthorized hardware or software?	**YES**	yes, this is part of Information Security Policy
Does your company have a formal, documented process or procedure that ensures information backup and recovery processes are in place?If YES: Describe the process or procedure.If NO: Provide business justification or any technical limitations. if N/A: Elaborate why this is not applicable.	**YES**	yes, this is part of Information Security Policy

Is business critical information backed up and capable of being recoveredin the event of hardware failures, data corruption, natural disasters or any other incident that is capable of destroying source data?	**YES**	The risk is managed by separating the storage ofproducion and back-ups on two separate servers, however in one phisical location. The cloud remote storage/virtual server is considered (not likely to be deployed before 2020)
Does your company have formal documentation that identifies the controls in place to effectively protect information resources against malicious code?	**YES**	Yes, information policy contains the details on both software and educational protection.
Do you have security tools installed that protect your information resources (desktops, laptops and servers) against malicious activity? (Security tools must detect, prevent, remove and recover from malicious activity conducted against your desktops, laptops and servers.)	**YES**	the corporate proxi server has antivirus McAfee and all local equipment also has antivirus installed (Microsoft Security Essencials, Windows Defender). All antivirus software is updated automatically realtime.

Are firewalls used when connecting your trusted network to an untrusted network?	**NO**	The compensatng set up is such that corporate router is configered by Cisco specialists (vendor) in such a way that it provides maximum protection/closedness from the outside environment and impossibility to connect from outside, this router configuration also has firewall functions/features enabled.
Are rules configured toallow only the appropriate traffic through?	**YES**	the access is granted or denied on the level of IP s of the outside sources
Are firewall rules reviewed and updated on a periodic basis to ensure only proper rules are set? (Reviews should be performed at least annually, and when significant changes occur.)	**YES**	IT specialist of Obriy and vendor (Cisco) - on "as needed" basis (any change management) but not less frequent than annually.

Are system, application and security logging enabled in production and non-production systems?	**NO**	most of the systmes and applications have their own internal activity logs. All VPN connections have activity logs. the activity on local PC or in terminal mode on server if not in the application is not logged. Compensating control - the rights to delete/modify files on the server while in terminal mode or on shared drive - are restricted.
Are logs reviewed on an as-needed basis based on risk and information classification of the application or system for which they are generated?	**YES**	based on user reports on any incidents or unusual behavior of certain system/application - the logs are reviewed, the issue is investigated and work toeliminate the threat is performed.
Does your company have formal documentation that identifies how you monitor and manage network traffic?	**NO**	the external traffic is monitored by means of corporate proxi server. The internal traffic is not monitored by any means, only manually on as needed basis.
Is network traffic monitored, controlled, managed and periodically evaluated to identify vulnerabilities?	**NO**	the external traffic is monitored by means of corporate proxi server. The internal traffic is not monitored by any means, only manually on as needed basis.

Do you perform network/server scans and penetration tests, using reputable products, to identify security gaps?	**NO**	as part of our PCI DSS related project we will have PAN -test (Performance Assessment Network Testing) performed by certified auditor. This test is aimed on identification of any vulnerabilities and will be performed annually as per the requirements.
Do you have documented processes in place to track and account for network devices, to ensure that only legal, licensed and approved IT assets are deployed in the environment throughout their lifecycle?	**NO**	it is prohibited to connect to the network with any non-approvedIT asset on the information security policy level, controled by line managers and any misuse is discoraged/prevented through presence of video survillance.
Is your network segmented between geographic regions, business units or critical assets to protect sensitive information?	**NO**	not yet, but within the PCI DSS related project the sensitive information will be separated into a dedicated segment
Is all end user access to the Internet conducted through a user proxy?If YES: Describe the controls.If NO: Describe any gaps and compensating controls.if N/A: Elaborate why this is not applicable.	**NO**	All appllications on the user desctop are configured to use proxy, however the user may tick "off" the proxy in the browser.

Is direct network access to Production and Non-Production servers restricted?	**YES**	from outside environment the access is restricted
Does your company have formal documentation that identifies the controls in place to effectively manage remote access to your information systems?	**YES**	Information security policy
Does your company have formal documentation that identifies the controls in place to effectively manage the segregation of duties?	**YES**	Information security policy and IS management plan
Do processes and controls incorporate the principle of "segregation of duties" in order to protect critical information resources?	**YES**	every system/application has its own users with the duty rights and roles. Total segregation of those roles which are connected with sensitive data (payment cards) is underway
Does your company have formal documentation that identifies the controls in place to effectively manage software patches and updates?	**YES**	Information security policy and IS management plan

Are software maintenance patches evaluated for applicability and implemented as appropropriate, with testing performed prior to installation?	**NO**	for number of systems/applications - we firstly test on staging platform (see IS management plan), for trusted vendors (like Microsoft or Cisco) - no testing prior to installation.
Are software maintenance patches received via a regular, established, automated process?	**YES**	for trusted vendors - viaautomated updates. On staging - on regular requests.
Do logged events include attributes (e.g., event ID, type, timestamp, etc.) to support security forensics and operational troubleshooting activities?	**NO**	only critical events in production systems are logged. Not all user activity.
Does your company have formal documentation that identifies the controls in place to effectively manage the configurations of operating systems and technology products throughout your environment?	**YES**	IS management plan

Do you have and utilize atest environment, in which software and integrations (new or modified) are tested in an environment outside of production?	**YES**	yes, Information policy provides the detail on testing procedures.
Is the test data used to perform software testing created from scratch, and not from production data?	**YES**	fake info is used
Are controls in place to ensure data used for testing will never be moved or copied into the production environment?	**YES**	separate databases and separate resources assigned
Do emails that you send as part of a service, to GBT or on GBT's behalf to other parties, utilize strong email authentication controls?	**NO**	the authentication is limited to the installation of the e-mail client and its configuration for appropriate user on a verified workstation. then the user is required to log into the workstation/desktop, on the e-mail client level the authentication of the user is not required.
Access Control		

Does your company have formal documentation that identifies how you manage access to information (i.e., access controls)?	**YES**	Information Security Policy
Are there rules or principles defined for assigning access to information systems (i.e. concept of least privilege, role-based, need-to-know)?	**YES**	role-based, the access is granted as per request of the line manager with the approval of asset/system owner
Are there controls in place that ensure access to information is approved or permitted by the information resource owner or delegate?	**YES**	the access is granted as per request of the line manager with the approval of asset/systemowner
Are there controls that ensure access to information is removed when it is no longer required?	**YES**	yes, the line manager`s obligation is to request the removal once no longer needed
Does your company have a formal, documented policy, process or procedure that ensures authentication credentials (e.g., passwords, passphrases, security questions/answers, PINs) are securely protected?	**YES**	Information Security Policy

Are controls in place to ensure systems or processes DO NOT support providing a copy of the password over the Internet using unsecured e-mail?	**NO**	secure transfer (paper-based) or internal e-mail traffic
Are digital signatures performed using an industry-appropriate algorithm and key length?	**YES**	For tax reporting application - the digital signatures are issued centrally by government authority
Does session-level encryption use Transport Layer Security (TLS)version 1.1 or higher, with an appropriate encryption algorithm and key length?	**YES**	
Are cryptographic controls used during the transmission of sensitive information?	**YES**	third party application (CIR)
Are cryptographic controls used during the storage and/or physical transport of sensitive information?	**YES**	for Payment card information -we have answer "yes" from PCI DSS compliant third party with no further detail available
Does your company have formal documentation that identifies the controls in place to effectively manage IDs used to access information systems?	**YES**	Information security policy

Are user access rights regularly reviewed and recertified, in an auditable manner, to confirm access is still necessary?	**YES**	manually, not less frequently than on a quarterly basis
Does your company have formal documentation that identifies the controls in place to effectively manage passwords for employee-facing systems?	**YES**	Information security policy
Are passwords, passphrases, PINs, and all other authentication credentials classified at your highest level?	**YES**	the user credentials are treated as secret information, separate sub-type of secret information is payment card information, all the rest of the information is either restricted (internal use only) or public. And the access to restricted information is role-based (+ elements of need-to-know)
Are there controls to ensure that authentication credentials are not shared with unauthorized parties or programmed into scripts or function keys?	**YES**	training, communications, internal guidelines

Are passwords • configured to be unique to the previous twelve (12) passwords? • restricted to eight (8) changes within a twenty four (24) hour period or one (1) calendar day -- except for one-time, single occurrence, or password vault implementations?	**NO**	different systems and levels of access have different authentication requirements
Do workstations & laptops which are used to store, process or transmit any sensitive information utilize whole disk encryption?	**NO**	bitlocker roll-out underway (by end of 2018)
Does your company have formal documentation that identifies the controls in place to effectively manage the locking of user interfaces?	**NO**	user training to lock the interface
Are there mechanisms in place to lock the user interface of a device after a period of inactivity?	**NO**	user training to lock the interface
Is re-authentication required when restoring access to a device interface?	**YES**	

Organizational Security		
Are supplier information security risk assessments performed for third parties that access, process, collect, create or store GBT information, and periodically thereafter based upon assessed risk?	**YES**	covered in contracts, the assessment is only made for PCI DSS vendors via tracking the certification validity
Is information created,stored and managed using only approved systems,equipment and software, with controls that ensure such information is used only for intended business purposes?	**YES**	Information security policy, job descriptions, NDAs with employees and contractors
Human Resource Security		
Are employees, contractors and third parties trained on their responsibilities for securing and protecting information resources?	**YES**	the policy is reviewed with new hires, the mandatory trainings are passed annually
Do individuals participate annually participate in and acknowledge review of information security training, and within 30 days of hire?	**YES**	

Incident Reporting and Management		
Does your company have formal documentation of principles that guide how you manage information security incidents?(e.g., a Security Incident Management policy)(Information security incidents shall be reported when discovered.)	**YES**	Information security policy
Asset Management		
Is a documented process or procedure in place to ensure sensitive information is identified and receives the correct label per your formal information classification scheme? (Personal Data (sometimes referred to as Personally Identifiable Information (PII) or personal information) is generally classified as GBT Restricted (or, external to GBT: as "sensitive").)	**NO**	the classification is simpleenough to treat info appropriatelywithout labeling. Cardinformation and any credentialsare secret. All the rest isrestricted if not public.

Does your company have formal documentation that identifies the controls in place to effectively manage information handling and disposal?	**YES**	Information security policy
Is sensitive information appropriately protected, according to its classification, as it is transported or stored using approved processes, solutions or third parties?	**YES**	the transmission of sensitive (payment card) information is by voice via non-recordable process, storage at PCI DSS compliant repository (CIR)
Are controls in place to ensure that your systems and/or processes prohibit the use of removable media?	**YES**	only several previledged users (approved by GM) may use removable media. Technical capability blocked for the rest. See information security policy.
Does your company have formal documentation in place that details requirements for ensuring all sensitive information has a designated custodian with defined responsibilities?	**YES**	Information security policy

Додаток Б

ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

ISO /IEC 27005 — міжнародний стандарт інформаційної безпеки, який в Україні має назву ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT), прийнято 18 грудня 2015 року, вступив в дію з початку2017 року.

Цей стандарт забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації.

Методи, описані в цьому стандарті, відповідають загальним поняттям, моделям і процесам, зазначеним в ISO / IEC 27001. Ці рекомендації призначені, щоб допомогти реалізувати достатню інформаційну безпеку, засновану на підході менеджменту ризиками.

Для закінченого розуміння цього стандарту важливо знайомство з поняттями, моделями, процесами і термінологією, описаної в ISO/IEC 27001 та ISO/IEC 27002.

Цей міжнародний стандарт є придатним до всіх типів організацій (наприклад, комерційні підприємства, урядові агентства, некомерційні організації), які мають намір здійснювати менеджмент ризиками, які ставлять під загрозу інформаційну безпеку організації.