ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

Пояснювальна записка

до бакалаврської роботи
на тему:

«КІБЕРБЕЗПЕКА ФАРМАЦЕВТИЧНОГО ПІДПРИЄМСТВА ЗАМКНЕНУТОГО ЦИКЛУ»

Виконав студент 4 курсу, групи СЗД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Систем інформаційного та кібернетичного захисту»
(шифр і назва спеціальності)

Дудник В.С
(прізвище та ініціали)

Керівник Шуклін Г.В.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Зозуля С.А.
(прізвище та ініціали)

КИЇВ-2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Систем інформаційного та кібернетичного захисту
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Систем інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
Шуклін Г.В.
«___»_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Дуднику Владиславу Сергійовичу
(прізвище, ім'я, по батькові)

1.Тема бакалаврської роботи: «Кібербезпека фарматевтичного підприємства замкненого циклу»

керівник бакалаврської роботи Шуклін Г.В., к.т.н, доцент кафедри
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «24 » лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 15 травня 2023 року

3. Вихідні дані до бакалаврської роботи

Об'єкт дослідження – є процеси технічного захисту інформації та процеси керування кібернетичними ризиками фармацевтичних підприємств закритого типу.

Методи дослідження – є методи системного аналізу та методи теоретико-порівняльного аналізу. Досліджуються ризики, які виникають на різних етапах підготовки фармацевтичних проектів.

Мета роботи – аналіз сучасних підходів щодо керування кібернетичними ризиками та розробка рекомендацій щодо забезпечення захисту інформації в фармацевтичних проектах підприємств замкнутого циклу.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

аналіз існуючих систем кібернетичного захисту фармацевтичних підприємств;

аналіз та дослідження технічних систем захисту в фармацевтичних підприємствах;

створення рекомендацій щодо застосування технічних систем в інформаційному захисті фармацевтичних підприємств.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Підбір науково-технічної літератури	до 20.02.23р.	виконано
2.	Обґрунтування актуальності теми роботи	до 27.02.23р.	виконано
3.	Написання першого розділу роботи	до 16.03.23р.	виконано
4.	Написання другого розділу роботи	до 12.04.23р.	виконано
5.	Написання третього розділу роботи	до 08.05.23р.	виконано
6.	Написання висновків по роботі	до 11.05.23р.	виконано
7.	Підготовка демонстраційних матеріалів	до 18.05.23р.	виконано
8.	Підготовка доповіді	до 24.05.23р.	
9.	Захист в ДЕК	до 20.06.23р.	

Студент _____ Дудник В.С.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Шуклін Г.В..
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина бакалаврської роботи: 55 сторінок, 3 рисунки, 6 таблиць.

Об'єкт дослідження – є процеси технічного захисту інформації та процеси керування кібернетичними ризиками фармацевтичних підприємств закритого типу.

Методи дослідження – є методи системного аналізу та методи теоретико-порівняльного аналізу. Досліджуються ризики, які виникають на різних етапах підготовки фармацевтичних проектів.

Мета роботи – аналіз сучасних підходів щодо керування кібернетичними ризиками та розробка рекомендацій щодо забезпечення захисту інформації в фармацевтичних проектах підприємств замкнутого циклу.

Для досягнення вказаної мети виконуються такі основні задачі:

аналіз існуючих систем кібернетичного захисту фармацевтичних підприємств;

аналіз та дослідження технічних систем захисту в фармацевтичних підприємствах;

створення рекомендацій щодо застосування технічних систем в інформаційному захисті фармацевтичних підприємств.

Новизна отриманих результатів полягає в наступному:

1. Розроблено алгоритм виявлення джерел несанкціонованого доступу до інформації в фармацевтичній сфері, а також розроблена система ідентифікації та аналізу киберризиків, які спроможні вплинути на реалізацію фармацевтичних проектів для фармацевтичних підприємств замкнутого циклів.

2. Розглянуті етапи життєвого циклу та визначена необхідність забезпечення захисту інформації при залученні консалтингових компаній.

Галузь використання – кібербезпека.

ABSTRACT

Bachelor’s thesis: 55 pages, 3 figures, 6 tables.

Object of research – of research: technical information security processes and cyber risk management processes of closed pharmaceutical companies..

Subject of research – methods of system analysis and methods of theoretical and comparative analysis. The risks that arise at different stages of preparation of pharmaceutical projects are investigated.

The purpose analysis of modern approaches to cyber risk management and development of recommendations to ensure information protection in pharmaceutical projects of closed-loop enterprises

To achieve this goal, the following main tasks are performed:

analysis of existing cyber security systems of pharmaceutical companies;

analysis and research of technical security systems in pharmaceutical companies;

development of recommendations for the use of technical systems in the information security of pharmaceutical companies.

The novelty of the results is as follows:

1. An algorithm for detecting sources of unauthorized access to information in the pharmaceutical sector has been developed, as well as a system for identifying and analyzing cyber risks that can affect the implementation of pharmaceutical projects for closed-cycle pharmaceutical enterprises.

2. The stages of the life cycle are considered and the need to ensure information security when engaging consulting companies is determined.

Field of use – cybersecurity.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СККР	Система керування кібернетичними ризиками	Cyber risk management system
ФП	Фармацевтичний проект	Pharmaceutical project
ІЗ	Інформаційний захист	Information protection
СЗІ	Система захисту інформації	Information security system
КСЗІ	Комплексна система захисту інформації	Comprehensive information security system
PKI	Інфраструктура публічних ключів	Public key infrastructure
RAM	Пам’ять з довільним доступом	Random Access Memory
RFID	Радіочастотна ідентифікація	Radio frequency identification
ROM	Пам’ять лише для читання	Read Only Memory
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	
ІТС	Інформаційно-телекомунікаційна система	
ОЗП	Оперативний запам’ятовувальний пристрій	
УВЧ	Ультра високі частоти	

ЗМІСТ

ВСТУП

Актуальність дослідження. пояснюється тим, що здійснення фармацевтичних проектів є достатньо конфіденційною процедурою і несанкціонований доступ до інформації, яка обробляється при реалізації фармацевтичних проектів може призвести до створення нових вірусів, нового виду озброєння, неспроможності підприємством вийти на ринок з новим лікарським засобом, який міг би допомогти багатьом хворим, тощо. Отже, надійний інформаційний захист (ІЗ) фармацевтичного підприємства замкненого циклу є запорукою миру та розвитком охорони здоров`я.

Велика кількість проектів щодо розроблення систем керування кібернетичними ризиками (СККР) у фармацевтичних проектах (ФП), або повністю не дає очікуваних результатів, або істотно потребує витрат додаткових ресурсів, а не тих які входили в бізнес планування. Однією з причин цьому, є відсутності в наявності вищого менеджменту та групи, які забезпечують виконання фармацевтичного проекту, функціонально стійких методів керування ризиками. Інакше кажучи, на теперішній час існує проблема коректного вибору та правильного застосування на практиці ФП інструментів керування кібернетичними ризиками, які пройшли апробування.

Об’єкт дослідження — процеси технічного захисту інформації та процеси керування кібернетичними ризиками фармацевтичних підприємств закритого типу.

Предмет дослідження —.

Мета роботи — аналіз сучасних підходів щодо керування кібернетичними ризиками та розробка рекомендацій щодо забезпечення захисту інформації в фармацевтичних проектах підприємств замкнутого циклу.

Завдання бакалаврської роботи:

— аналіз існуючих систем кібернетичного захисту фармацевтичних підприємств;

— аналіз та дослідження технічних систем захисту в фармацевтичних підприємствах;

— створення рекомендацій щодо застосування технічних систем в інформаційному захисті фармацевтичних підприємств

Методи дослідження – методи системного аналізу та методи теоретико-порівняльного аналізу. Досліджуються ризики, які виникають на різних етапах підготовки фармацевтичних проектів.

Новизна отриманих результатів полягає в наступному:

1. Розроблено алгоритм виявлення джерел несанкціонованого доступу до інформації в фармацевтичній сфері, а також розроблена система ідентифікації та аналізу кіберризиків, які спроможні вплинути на реалізацію фармацевтичних проектів для фармацевтичних підприємств замкнутого циклів.

2. Розглянуті етапи життєвого циклу та визначена необхідність забезпечення захисту інформації при залученні консалтингових компаній.

1 ОСНОВНІ ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ФАРМАЦЕВТИЧНИХ ПІДПРИЄМСТВ ЗАМКНЕНОГО ЦИКЛУ

1.1 Захист інформації при здійсненні логістичних операцій

Основним завданням логістики є мінімізація витрат, за винятком операцій, пов`язаних з інформаційною безпекою та захистом інформації, а також організаційного та функціонального змісту, що є невід`ємною частиною стійкого функціонування підприємства.

Керівник фармацевтичної компанії спроможний здійснювати прозоре керування інформаційно-матеріальними потоками діяльності суб'єктів фармацевтичного ринку при існуючій динаміці попиту та стану ринку ліків.

Об'єкти логістики - матеріальний, фінансовий, інформаційний та сервісний потоки на всьому шляху руху - від первинного джерела сировини до кінцевого споживача.

Завдання логістики полягає в контролі проходження матеріального потоку через ланцюг руху процесів, пов`язаних з поставками, а саме – контроль за підприємствами, завдяки яким відбувається проходження фармацевтичних матеріалів під час свого переміщення від постачальників початку циклу до кінцевого споживача.

На рисунку 1.1 представлено три напрямки розвитку логістики, де кожний з них має свої слабкі місця, щодо захисту конфіденційної інформації.

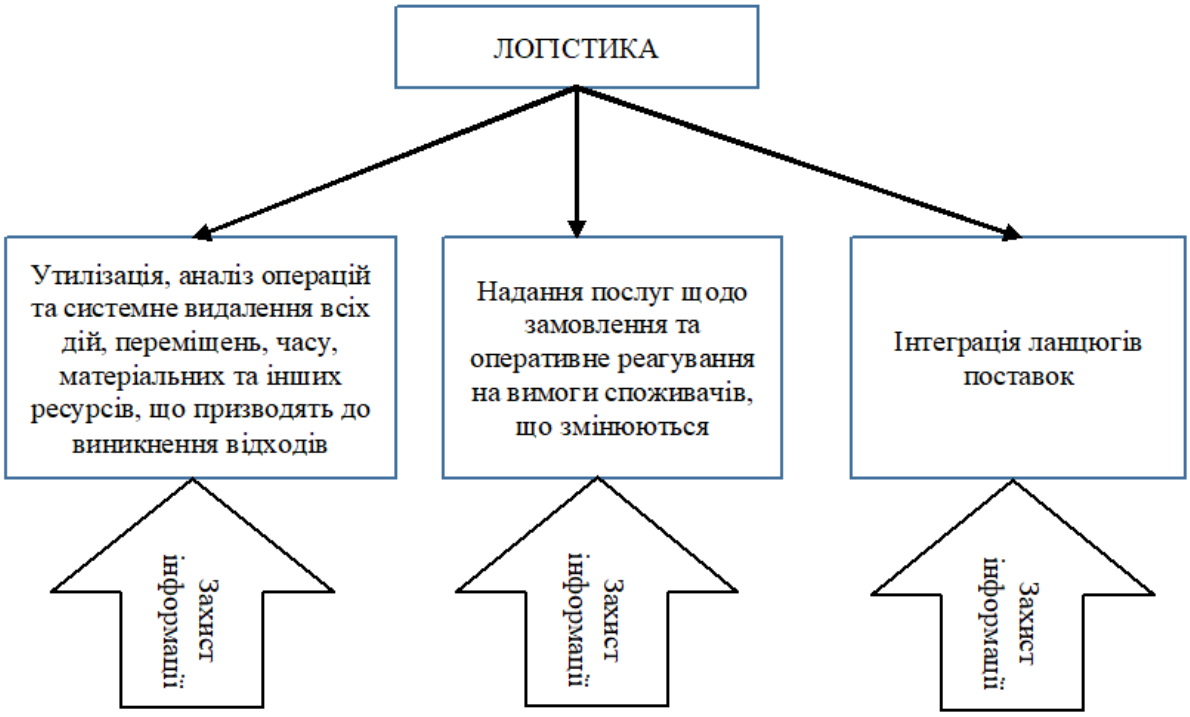

Рисунок 1.1. Три напрямки розвитку логістики, які потребують ІЗ.

Так як всі логістичні витрати включають в себе витрати на переміщення, складування, керування запасами, пакування, обробку конфіденційної та комерційної інформації, то захист інформації від сторонніх очей є достатньо не простою задачею. При системному підході щодо забезпечення логістичних дій, всі взаємопов'язані логістичні операції здійснюються узгоджено, зниження витрат на певний тип операції породжує зниження всіх логістичних витрат, при цьому витрати на іншу операцію, не пов`язану з логістикою, можуть збільшуватись.

Кожне підприємство розробляє свій власний логістичний алгоритм, який враховує усі стратегічні рішення, включаючи і захист конфіденційної операції, який повинен постійно здійснювати контроль від можливого витоку як по технічним каналам так і за рахунок інсайдерів. На теперішній час використовують дві базові в інформаційному захисті: тонка та динамічна.

Метою "тонкої" стратегії є мінімізація загальних витрат на кібернетичний захист, гарантуючи при цьому номінальний рівень інформаційного захисту.

Метою динамічної стратегії є забезпечення високого рівня ІЗ, оперативне реагування на появу нових джерел несанкціонованого втручання в технічні канали або моніторинг існуючої системи захисту з подальшою її модернізацією, якщо це необхідно.. Динамічна стратегія сфокусована зовнішніх джерелах несанкціонованого зняття інформації по технічним каналам.

Керування ризиками інформаційного витоку при здійсненні логістичних операцій базується на методі залучення окремих взаємопов'язаних елементів системи інформаційного захисту в інтегрований процес бізнесу з метою запобігання несанкціонованого витоку за рахунок інсайдерів. На рисунку 1.2 представлено операції, які потребують інформаційного захисту.

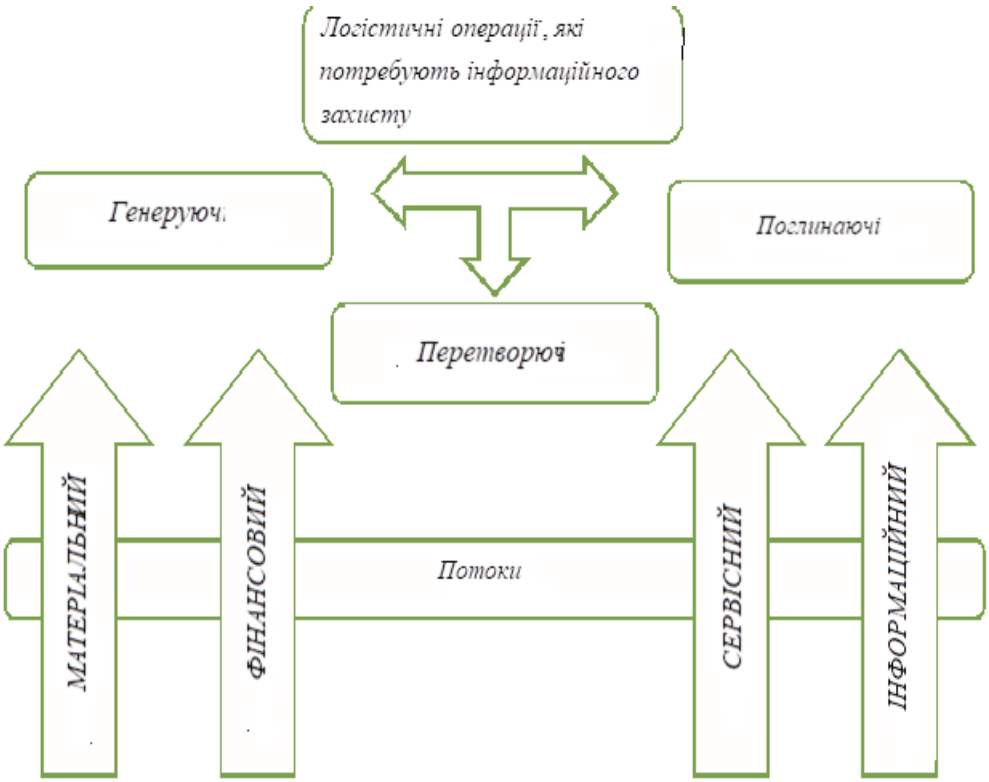

Рисунок 1.2. Логістичні операції фармацевтичного підприємства замкненого циклу, які потребують інформаційного захисту.

Систему інформаційного захисту можна розділити на систему захисту макрологістичних операцій - це потужна система керування ІЗ для забезпечення стійкості матеріальних потоків, які охоплює фармацевтичне підприємство, посередницькі, торговельні та транспортні компанії, які зосереджені в різних регіонах країни або за її межами.

В процесі формування макрологістичних операцій важливим є подолання складнощів, які виникають за рахунок правових та економічних складових міжнародних економічних відносин, з нерівними умовами постачання товарів, відмінностями в транспортному законодавстві країн, а також низку інших інформативних завад. На рисунку 1.3 представлено складові макрологістичної системи, які потребують інформаційного захисту.

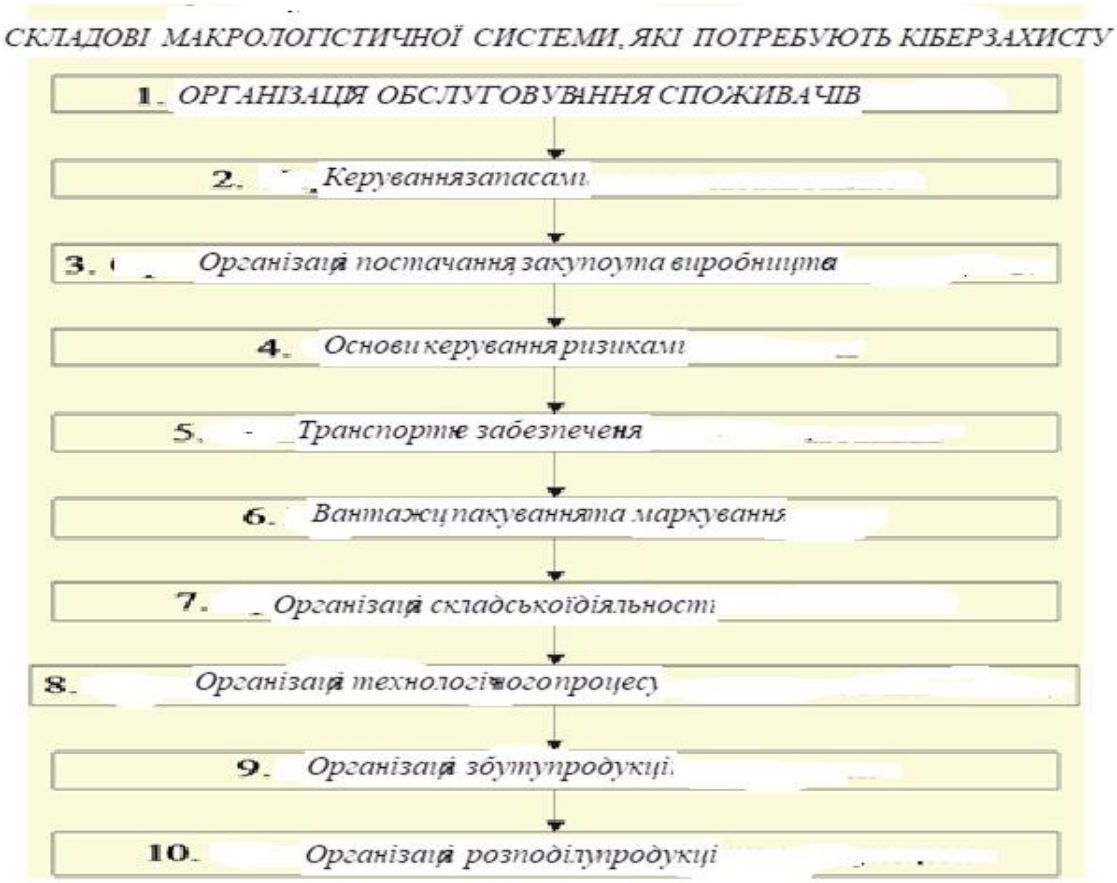

Рисунок 1.3. Складові макрологістичної системи, які потребують ІЗ.

Формування систем захисту інформації (СЗІ) у міждержавних програмах вимагає створення єдиного кібернетичного простору.

Мікрологістичні операції є підопераціями, структурними складовими макрологістичних операцій. До таких відносяться відмінні виробничі та торговельні компанії. Мікрологістичні операці уявляють собою групу внутрішньовиробничих кібернетичних систем, до складу яких входять технологічно пов'язані виробництва, об'єднані єдиною інфраструктурою.

Кібернетична система формулює та розв'язує завдання проектування комплексних систем захисту інформації (КСЗІ), узгоджених матеріальних потоків із заданими характеристиками на виході. Ця система відмінна від інших високим рівнем узгодженості системи захисту, що включаються до них, з метою керування інформаційними ризиками логістичних операцій.

1.2. Функціональна стійкість системи захисту логістичних операцій

Система інформаційного захисту має інтегративні властивості, не властиві жодній з її складових. Це спроможність здійснити моніторинг непідробного товару, коли в необхідний час необхідно доставити в потрібне місце з найменшими витратами, а також спроможність адаптуватися до можливих намагань отримати несанкціонований доступ з зовнішнього середовища. Моделювання системи захисту інформації подібна системам масового обслуговування і характеризується в першу чергу внутрішнім станом системних зв'язків і зв'язками із зовнішнім середовищем. Внутрішні системні зв'язки під час надходження інформаційного потоку мають властивість циклічності, а обробка внутрішнього інформаційного надходження відбувається за схемою послідовного аналізу. Зв'язки системи захисту інформації із зовнішнім середовищем мають циклічні та синергетичні властивості.

Передумовами для інтегрованого підходу в системі захисту інформації є:

у нове розуміння механізмів створення загроз та логістики як стратегічного елемента в реалізації та розвитку конкурентних можливостей підприємств;

у реальні перспективи та сучасні тенденції щодо інтеграції учасників інформаційного простору, які зв'язані між собою, розвиток нових організаційних форм - мереж систем захисту;

у технологічні можливості в галузі інноваціних інформаційних технологій, що відкривають принципово нові можливості для взаємодії та зниження витрат.

Основна діяльність служби захисту інформації фармацевтичного підприємства спрямована на регулювання та координацію різних вхідних і

вихідних інформаційних потоків, таких як матеріальний. Взаємозв'язок систем інформаційного захисту із зовнішнім середовищем показано на рисунку 1.4.

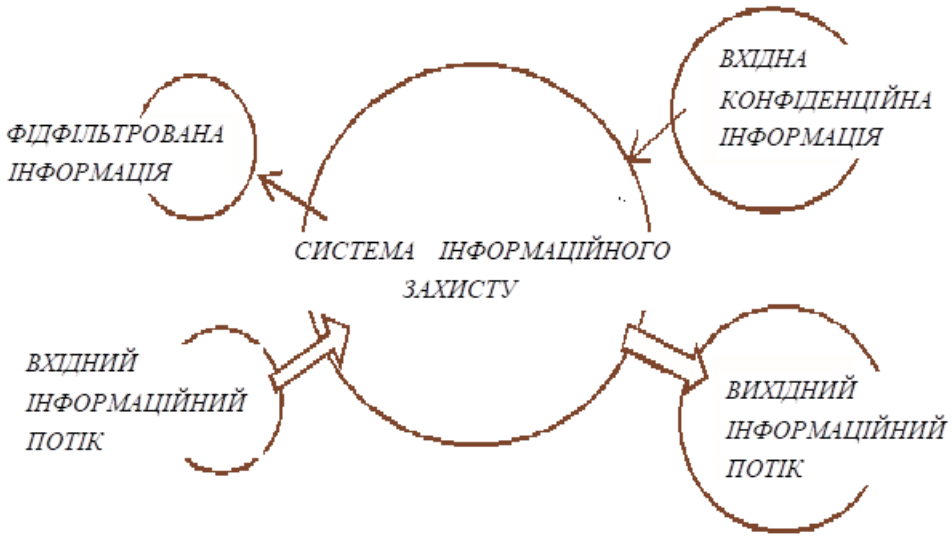

Рисунок 1.4. Взаємозв`язок системи ІЗ з зовнішнім середовищем

Система інформаційного захисту має чотири основні властивості:

1. Властивість цілісності та член.

Цілісність - система є цілісна сукупність елементів, що взаємодіють один з одним. Декомпозицію логістичних систем на елементи можна здійснювати по-різному, залежно від рівня: на макрорівні при проходженні матеріального потоку від одного підприємства до іншого як елементи можуть розглядатися самі ці підприємства, а також транспорт, що їх зв'язує; водночас на мікрорівні логістична система може бути представлена у вигляді підсистем закупівлі, збуту та управління виробництвом.

- На макрорівні:

1.3. Роль оператора кібернетичного захисту в ланцюгу фармацевтичного підприємства замкненого циклу

Фармацевтичний оператор захисту інформації уявляє собою інтегратор процесів захисту інформації високого рівня, коли ланцюжок захисних заходів контролюється та керується захисним провайдером, та функції якого націлені на виконання послуг з технічного захисту та керування системами захисту. На рисунку 1.5 представлено загальну схему фармацевтичного оператора.

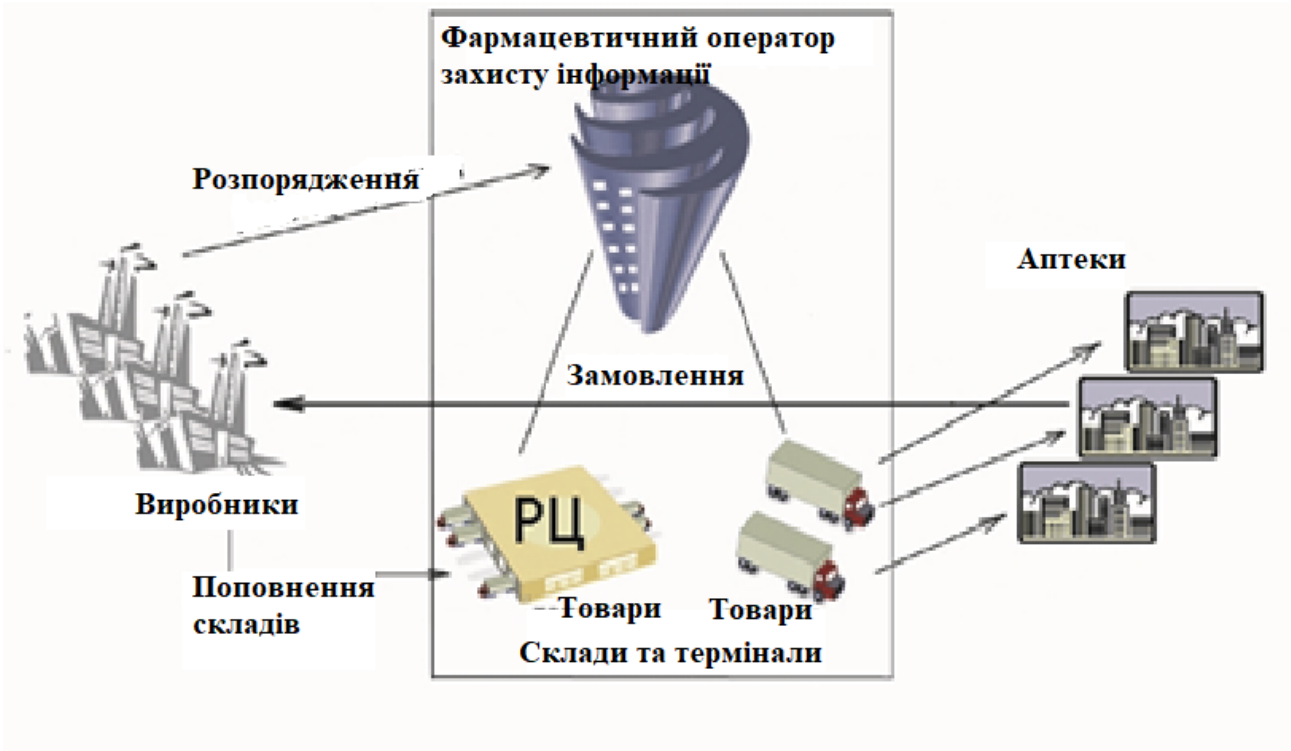

Рисунок 1.5. Загальна схема фармацевтичного оператору захисту інформації

На рисунку 1.6 представлено схему єдиного інформаційного простору.

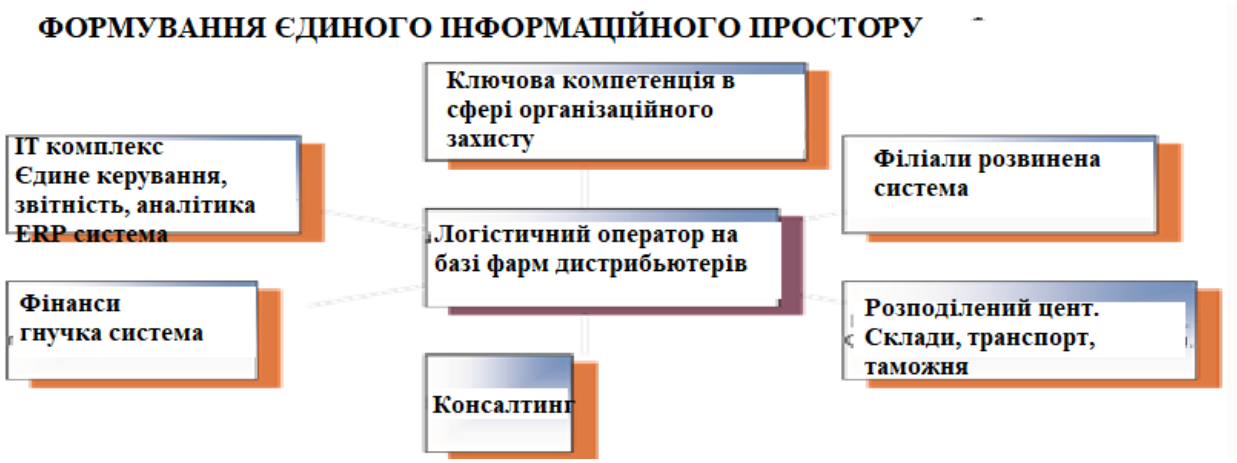

Рисунок 1.6. Структурна схема єдиного інформаційного простору

З рисунку 1.6 видно, що фармацевтичне підприємство замкненого циклу потребує особливого інформаційного захисту, особливо від інсайдерів, а також від тих технологій, які фармацевтичне підприємство впроваджує. На рисунку 1.7 представлено схему ризиків самої логістичної системи.

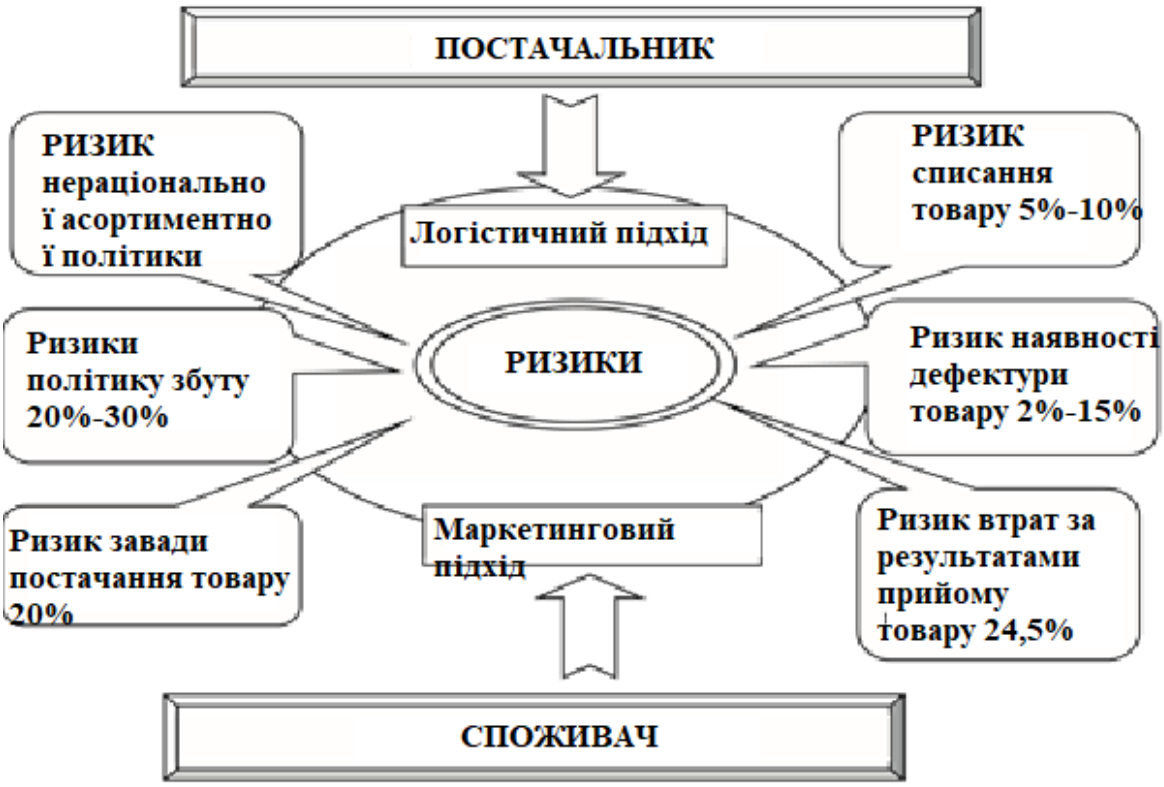

Рисунок 1.7. Схема ризиків логістичної системи

З рисунку 1.7 видно джерела виникнення ризиків. Кожен з джерел має свої особливості, які в першу чергу пов`язані з людськими факторами.

Висновки до першого розділу

1.Фармацевтичні підприємства замкненого циклу мають багато слабких місць, пов`язаних з їх діяльністю. Це пов`язано з тим, що саме ця галузь постійно підлягає спотворенню від конкурентів.

2.Для того, щоб здійснити забезпечення інформаційного захисту підприємств даної галузі, необхідно в першу чергу розуміти, який інформаційний захист, крім захисту периметру ОІД , дані підприємства потребують.

РОЗДІЛ 2 КЕРУВАННЯ КІБЕРРИЗИКАМИ В ФАРМАЦЕВТИЧНИХ ПІДПРИЄМСТВАХ

2.1 Огляд існуючого термінологічного апарату

Велика кількість проектів із розроблення систем керування кіберризиками (СККР) у фармацевтичних проектах, або повністю не призводить до очікуваних результатів, або істотно вимагає втрат більших ресурсів, ніж це виносилось на планування. Одна з причин такого явища, є відсутність в розпорядженні головного менеджменту та учасників проекту надійних методів керування ризиками. Більшою мірою це твердження справедливе щодо коректного вибору та мудрого застосування в практиці фармацевтичних компаній апробованих інструментів керування кіберризиками.

В даній роботі представлено підхід для фармецевтичного підприємства замкненого циклу, в якому здійснювалось розроблення системи керування кіберризиками. Певну увагу приділено залученню консалтингових компанія до діяльності фармацевтичного підприємства, розглянуто реалізацію даного підходу. Запропоновано систему вибору та застосування різних інструментів керування кіберризиками на всіх стадіях життєвого циклу фармацевтичних підприємств закритого циклу.

Для досягнення мети в даній роботі було досліджено в першу чергу відповідний термінологічний апарат для формування зрозумілих сутностей та аналізу їх взаємозв'язків у проекті систем керування кіберризиками стосовно галузі фармацевтичних підприємств. Запропоновано таке визначення фармацевтичного проекту, як діяльність фармацевтичної компанії в межах угоди про розподіл продукції, концесійної угоди, угоди про засади проведення хімічного складу вивчення препараті, які виробляються, меморандуму, протоколу, угоди про спільну діяльність та інших угод у сфері клінічних досліджень нових препаратів.

Зрозуміло, що мають бути взяті до уваги не тільки класичні джерела, такі як а й низка експертних майданчиків, здатних допомогти у формуванні узгодженої термінології. Одним з таких розбіжностей в термінології присутні в нормативних документах України зокрема, для термінів модель , ДСТУ Р ІСО/ТО 15879-2008, ДСТУ Р 48796-2009, стандарт ДСТУ Р 74589.2-2018 та інші.

Пропонується як " " узяти описи бізнес-процесів, які націлені на отримання доданої вартості. Це стосується не тільки по відношенню до зовнішнього споживача. Варто зазначити, що бізнес-процес, як актив високої ціни сучасних проектів, який має наближення до ризиків особливо до до кіберризиків.

Українсько-американський словних термінологій по кібербезпеці, створений Інститутом інформаційної безпеки та EastWest Institute (США), говорить, що кібербезпека, є властивістю кіберпростору, яка протистоїть навмисним та ненавмисним загрозам, а також реагує на них та відновлення після їхнього впливу. Проте, визначення кіберризиків відсутнє. В іншому підручнику, надається визначення поняття кібербезпека, як наступне: Кібербезпека – це діяльність або процес, здатність, можливість або стан, за яких системи інформації та зв'язку й інформація, що міститься в них, захищені та/або охороняються від шкоди, несанкціонованого використання, модифікації або експлуатації. Також, в тексті згадуються кіберризики, проте точного визначення не надано. Компанія Gartner надає визначення кібербезпеки з огляду позначення практичних методів безпеки, що в собі поєднали заходи наступального й оборонного характеру, як сукупність системи інформаційних та/або операційних технологій. Зазначино, що визначення кіберризиків, також відсутнє.

В документі ITU-T Recommendation X.1205 "Overview of cybersecurity" визначення кібербезпеки, має наступне значення, це набір інструментів, політик, концепцій, заходів захисту, підходів ризик-менеджменту, навчання, найкращих практик, технологій для захисту активів користувача та організацій. Зазначино, що в даному документів зазначино підходи ризик-менеджменту, але більш чіткого визначення немає.

У документі "Cybersecurity Supervising a Moving Target", який містить рекомендації відносно фінансової сфери, детальних рекомендацій до управління кібербезпеки не має. Присутні, тільки загальні відомості, що кіберризики характеризуються відсутністю будь-яких стандартів і настанов і відображено точку зору, що кіберризиками можна керувати, але ніколи не можна виключити. Даний документ немає необхідних інструкцій. Тому, введимо нове визначення кіберризику - ризик, пов'язаний із використанням технологій, обладнання та програмного забезпечення (ПЗ), зокрема під час управління НГП. Для оцінки кіберризиків застосовують різні стандарти.

2.2.Проблемна сфера та підходи захисту інформації в фармацевтичних підприємствах

Власники бізнес-процесів, зазвичай потребують від спеціалістів опис проблемних ділянок, у даних процес не завжди досягають мети та відповідно можливі втрати. Розуміємо, під терміном «витрати» не тільки фінансові втрати. У НГП визначено порядок, порушення якого (і рівною мірою поява загроз порушення) має попереджатися спеціальними процедурами (у рамках систем менеджменту) ще "на підході". Дані системи розглядаються, як системи менеджменту інформаційної безпеки (ISO 27001), системи менеджменту безперервності бізнесу (*ISO*22301), системи менеджменту IT-послуг (ISO 20000:1) та інтегрованих систем менеджменту (ICM). Тому, визначино проблемні області:

1. Зрив термінів виробничих завдань. Нові можливості, створюють і нові ризики, які включають кіберризики.

2. Великі IT, у яких працюють багато співробітників, розширюють проблеми кіберризиків, наприклад, поява єдиної точки відмови.

3. Складне обладнання у використанні.

Розглянуто, кілька підходів СУКР, як рекомендації для НГП:

1.Стандарти ISO. Впроваджують переважно підприєства харчової промисловості.

2. Уніфікація стандартів.

3. Підхід NASA, модель «цифрових двійників», застосовує віддзеркалювану інформацію під час управління складними об'єктами впродовж усього життєвого циклу), методи машинного навчання та статистичного моделювання. Найбільше значення мають "операційні двійники", але це потрібно Пфлопс на серверах високої продуктивності.

4. Рішення класу GRC (Governance, Risk, Compliance), запропоновані розробниками (наприклад, RSA, Oracle, SAP, RVision), проте широкого застосування даний підхід немає.

5.Методики ISAGO, ITIL, COBIT, Octave, RiskIT, Harmonized TRA Methodology, увага звертається забезпеченню ІБ, але єдиного рішення, пов’язаних із ЖЦ не має.

Відомі компанії пропонують власні рішення, але це також не має конкретних рішень.Проте, навіти при виборі консультантів можуть бути враховані не всі фактори. Потрібно, брати до уваги раніше визначені «проблемні області», які розглянемо далі.

2.3. Некеровані ризики інформаційного захисту в фармацевтичних підприємствах

Маючи досвід із реальним проєктом фармацевтичного підприємства, представлено значущі ризики:

1.Виявлення, ідентифікація та оцінювання кіберризиків. Ввідомі компанії представили рішення по раніше виявлених проблемах.

2.Кіберризики, які потребують управління.

3. Управління кіберризиками. Потрібно, витрачати, якомого менше часу на усунення наявних кіберризиків.

Далі, розглянуто кейси, які виявлені в НПГ.

Certificate of Achievement

This is to certify that

[redacted]

has successfully completed the course assessment and examination for the

ISO 9000:2000 Series Auditor/Lead Auditor Training Course

which is certified by the Governing Board of the Institute of Quality Assurance (IQA), International Register of Certificated Auditors (IRCA) and is compliant with the training requirements of the International Auditor and Training Certification Association (IATCA) for certification as an

IATCA QMS Auditor/Senior Auditor

and as an

IRCA QMS Auditor/Lead Auditor and Internal Auditor

Held on: 24th – 28th February 2003 at: Moscow, Russia

Signed: Training Manager Date: 27 May 2003

Certificate Serial No: LA2/03/RU/2519 Course Certification No: A 17024

IATCA

Рисунок 2.1. Приклад "сертифіката" експерта на відповідність словнику ISO 9000 (ISO 9000 ствий), і опис одного з бізнес-процесів, у яких є входи, але немає виходів

Розглянемо приклад порушення політики «чистий стіл і чистий екран», як це зображено на рисунку 2.2.

Рисунок 2.2. Залишені документи

Залишені документи, включаючи, ті що містять конфіденційну інформацію, незаблоковані комп'ютер та смартфон, доступ до приміщення є в більшості співробітників (враховуємо і потенційних клієнтів).

Спершу, потрібно оцінити рівень зрілості співробітників та прийняти рішення, який інструмент потрібно застосувати.

Інструменти ризк-менеджменту

Враховуючи, минулий досвід, команда прийняла рішення про створення СУКР в складі стандартів ISO серііі 9001, 14001, 27001, 19011, 31000,38500 та 37000.

Визначино, що потрібно два інструменти при реалізації НГП в компанії холдингового типу:

1.«Менший набір»: ISO 31000 (31010) версії 2018 (2019), ISO/IEC 27005 версії 2018 та NIST SP-800-53.

2. «Більший набір» - для забезпечення подальшого розвитку СУКР:

ISO серії 19011 – для виконання аудитів;

ISO серії 31000 (31010) – для управління ризиками;

ISO серії 38500 – для управління IT;

ISO серії 37000 – для управління аутсорсінгом.

Управління кіберризаками в фазах циклу PDCA

Всі пропозиції, заявлені командою НГП, перевіряються в повній мірі протягом планового внутрішнього аудиту з встановленою періодичністю.

Повністю перевіряється визначення внутрішнього та зовнішнього контексту, та всі комплексіні технічні рішення і засоби забезпечення ІБ відповідно до раніше встановлених цілей НГП. Застосовано раніше пропоновані рішення, для системного редагування внутрішньої нормативної документації та перерозподіл ресурсів. Приклад СуКР реалізовано в фазі Check цикла Демінга.

Враховуючи, негативний досвід роботи консультантів, розробка СУКР був визначений, як системний підхід при виконанні НГП, як це представлено на рисунку 2.3.

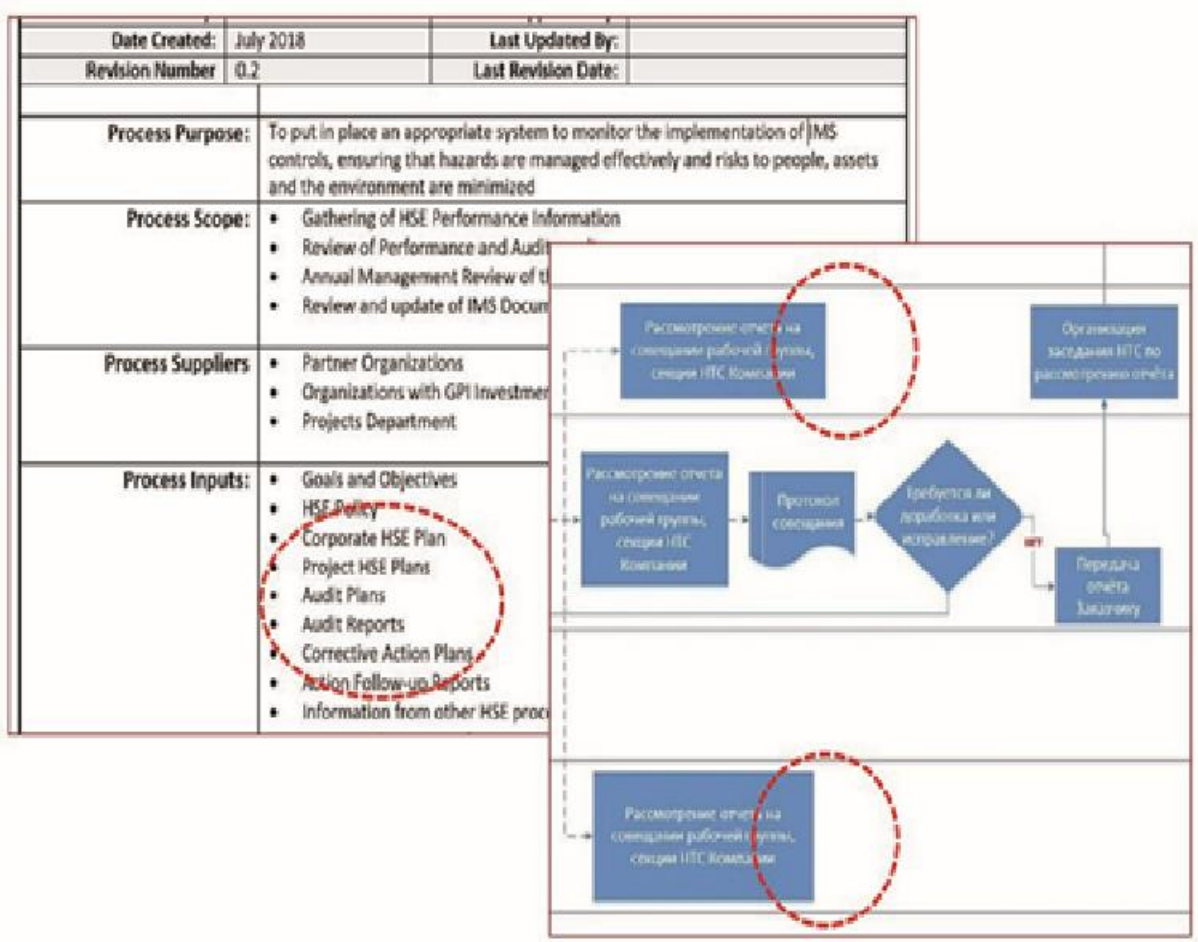

Рисунок 2.3. Приклади стандартних рішень консультантів

Висновки до другого розділу

1.Головним завданням захисту інформації фармацевтичного підприємства закритиго циклу полягає в безперервному процесі виявлення кіберактивів. Процес усунення "*сліпих зон*" здійснюється засобами безперервного пошуку та виявлення як внутрішніх, так і зовнішніх (*з виходом в інтернет*) відомих і невідомих активів. Автоматизована ідентифікація та профілювання динамічної поверхні кібератаки створюють спроможність отримати постійно оновлюваний перелік кіберактивів з інформацією, що необхідна для оцінювання рівня ризику та схильності до нього.

2. Процес виявлення критичних ризиків полягає в оцінці корпоративних ризиків в загалом та фіксацією конкретних факторів та особливостями ризику - критичністю активів, вразливостями, рівнем інформаційної системи захисту, активністю загроз і схильністю до ризику.

3. Для визначення пріоритетних інновацій та дій, необхідних для підвищення рівня інформаційного захисту, необхідно застосовувати автоматизоване оцінювання ризиків, аналіз тенденцій та порівняння з галузевими показниками.

4. При забезпеченні захисту інформації фармацевтичних підприємств необхідно створювати дії на випередження. Для цього необхідно постійно здійснювати усунення ризиків з подальшим зниження ймовірності компрометації даних.

5. Необхідно постійно спиратися на інсайт, отриманий на основі інтелектуальної та тактичної інформації щодо ризиків.

6. Необхідно постійно отримувати домінуючі рекомендації щодо зниження рівня ризиків з подальшою швидкою автоматизацією та миттєвим реагуванням на ризики в масштабах усього фармацевтичного підприємства закритого типу.

3 ІНСТРУМЕНТИ РИЗИК-МЕНЕДЖМЕНТУ В ФАРМАЦЕВТИЧНИХ ПІДПРИЄМСТВАХ

3.1 Керування ризиками несанкціонованого доступу до інформації в режимі PDCA

Потрібно враховувати реалізацію територіально розприділених, технічно та технологічно складних НГП в обмеження зовнішніх негативних впливів. Власник НГП потребує забезпечити досягнення цілей проєктної команди, при цьому забезпечити якість реалізації НГП. «Якість реалізації» відноситься до широкого спектру, в тому числі,аспекти ІБ. Важливим фактором, являється не розділена «локальні» цілі і потім досягнення «глобальних» цілей для всього НГП у компанії холдингового типу, а побудова ІСМ, у якій забезпечується досягнення єдиної мети, з урахуванням, відповідно, всіх відомих раніше обмежень, що обурюють впливів, і, безумовно, – сукупності ризиків під керівництвом СУКР (див. рис. 3.1). Представлено додаткові пояснення, в основному різниця між поняттям «система управління» і «система менеджменту», які зазвичай мають складність в практичному застосуванні.

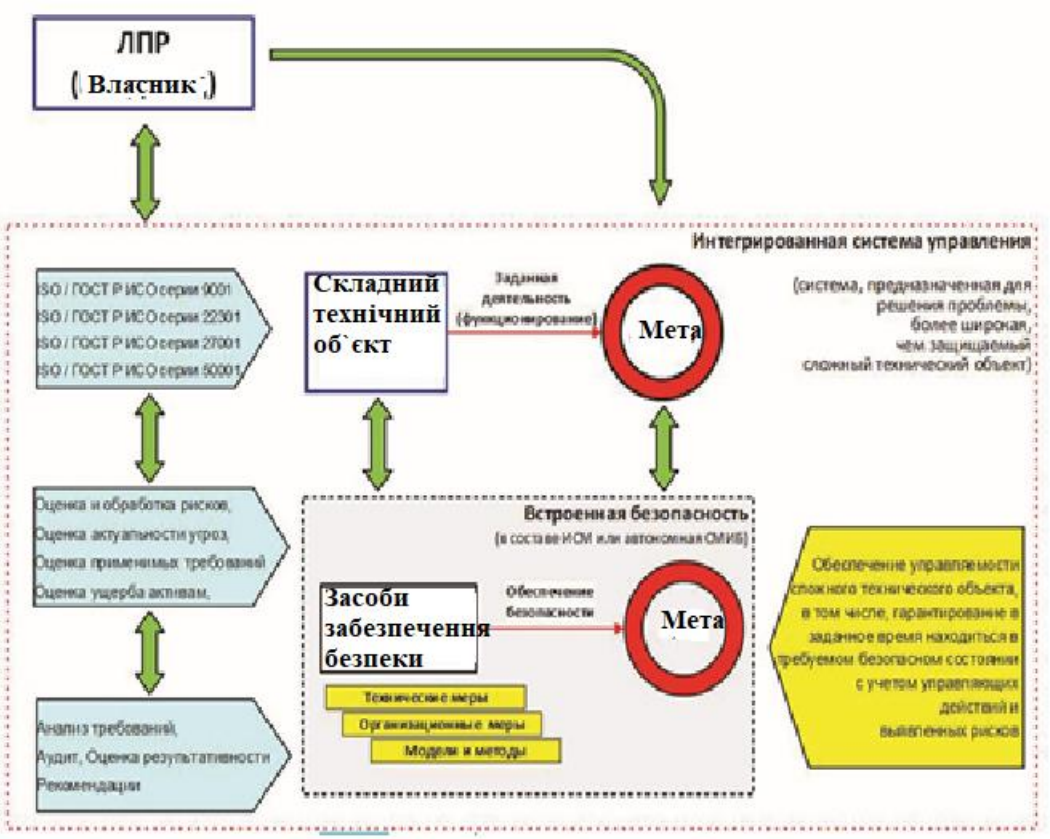

Рисунок 3.1. Керування ризиками

Таблиця 3.1.

Різниця між системою керування та системою менеджменту

Сутність	**Система управління**	**Система менеджменту**
Реалізація об’єкту	СУ (Інтегрована СУ)	Система менеджменту якості Система менеджменту безперервності Система менеджменту ІБ Система менеджменту ІТ-сервісів ІСМ (інтегрована)
Обмеження	ЛПР (директор)	Керівники функції (процесу) Представники керівництва (ПРК,..)
Досягнення мети	Бізнес-цілі	Відповідність вимогам чинного законодавства Виконання критичних факторів успіху (KPI)
Вимоги	Бізнес	PCI DSS, GDPR та ін.
Підхід до управління	Застосування бізнес-практик	Оцінка ризиків Найкращі існуючі технології Галузеві рекомендації (вимоги)

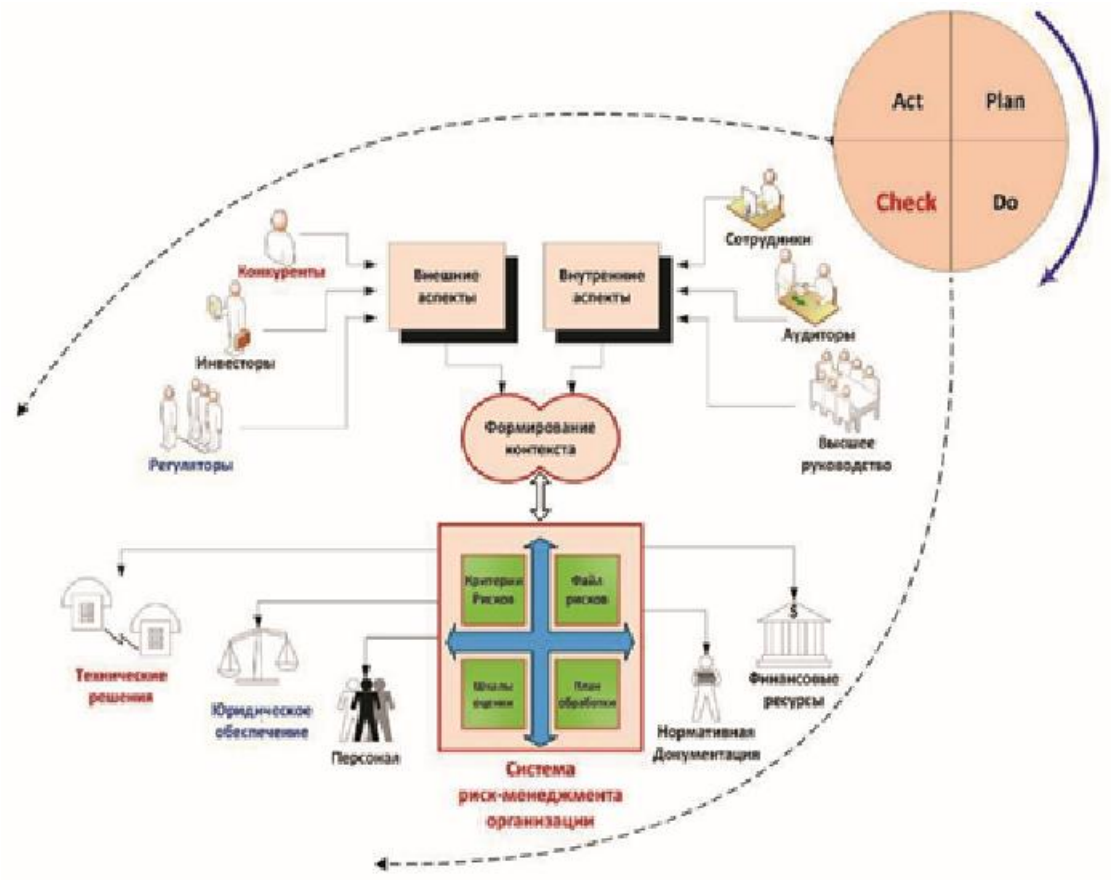

Рисунок 3.2. Система циклічності в системі захисту

3.2. Інтегровані системи менеджменту

На практиці застосовується «єдине управління» для забезпечення успішної діяльності компанії, а також облік кращої практики. Зазначино, що в проєктній НГП приділяється більше уваги сучасним вимогам стандартів ISO. Успіх в розглянутій НГП являється, те що застосовується підтримка сучасної IT. Відповідно, були доповнені вимоги щодо забезпечення ІБ, особливо при поділі передачі інформації між внутрішнім і зовнішнім периметром. Особлива увага приділена досягненню ефекту емерджентної системи - органічної інтеграції всіх робочих органів компанії в "єдине керуюче поле". Тому, формується умови для створення ефективної корпоративної СУКР, яка впливає на НГП.

Створення сучасної СУКР, яка розроблена для забезпечення управління НГП, значно відрізняється від інших задач. Слід забезпечити облік значної кількості факторів, у стандартах ISO, які називаються «зовнішнім контекстом» та

«внутрішнім контекстом», та забезпечити підтримку ІСМ за допомогою СУКР. Аналіз показує, що система ризку-менеджменту не може існувати окремо від ІСМ. У забезпечення цієї тези можна привести достатньо пропозицій від компаній (IBM, EMC, RSA, SAP, Oracle тощо), і заслуговує на особливу увагу пропозиція нових підходів, званих «цифровими двійниками».

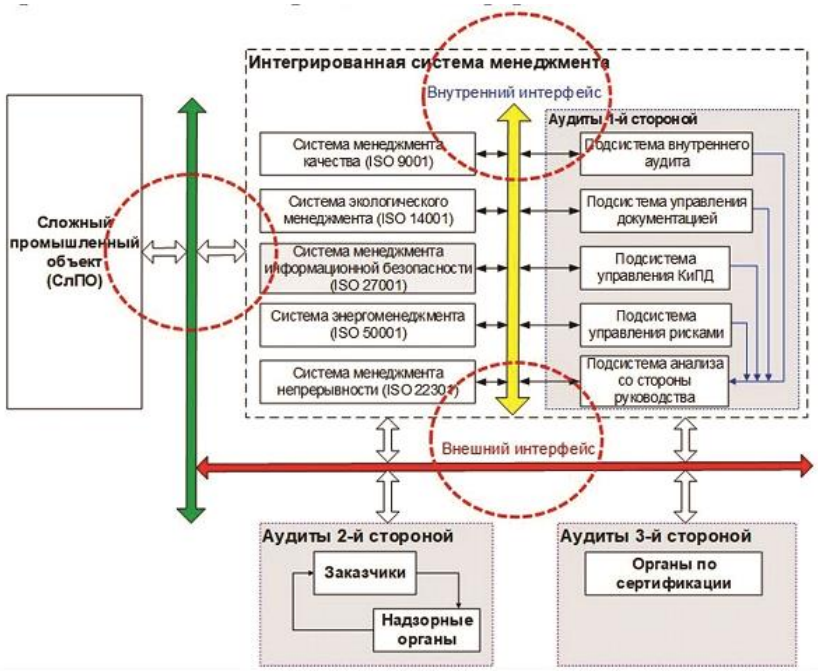

Рисунок 3.3. Розділення інформації на підприємстві

В роботі СУКР було реалізовано нову межу інтеграції, кіберризики були інтегровані в «єдине управліннське поле» компанії при виконанні НГП. Застосування стандартів ISO/IEC серії 27001 або 20000 являється недостатнім і потрібно застосовувати більш сучасні.

При створенні СУКР для виконання НГП в компанії холдингового типу необхідно створювати ІСМ у складі відомих стандартів ISO серії 9001, 14001, 27001, 45001 та ін., а також враховувати нові перспективні стандарти ISO, наприклад, серії 37500, 38500 і 30401. Ці вимоги повинні бути максимально враховані у консалтингових компаніях, для яких процедури управління кіберризками повинні встановлюватися і контролювати з ранньої стадії ЖЦ.

Отже, в роботі зображено загальні результати, отримані практичним підтвердженням при реалізації НГП.

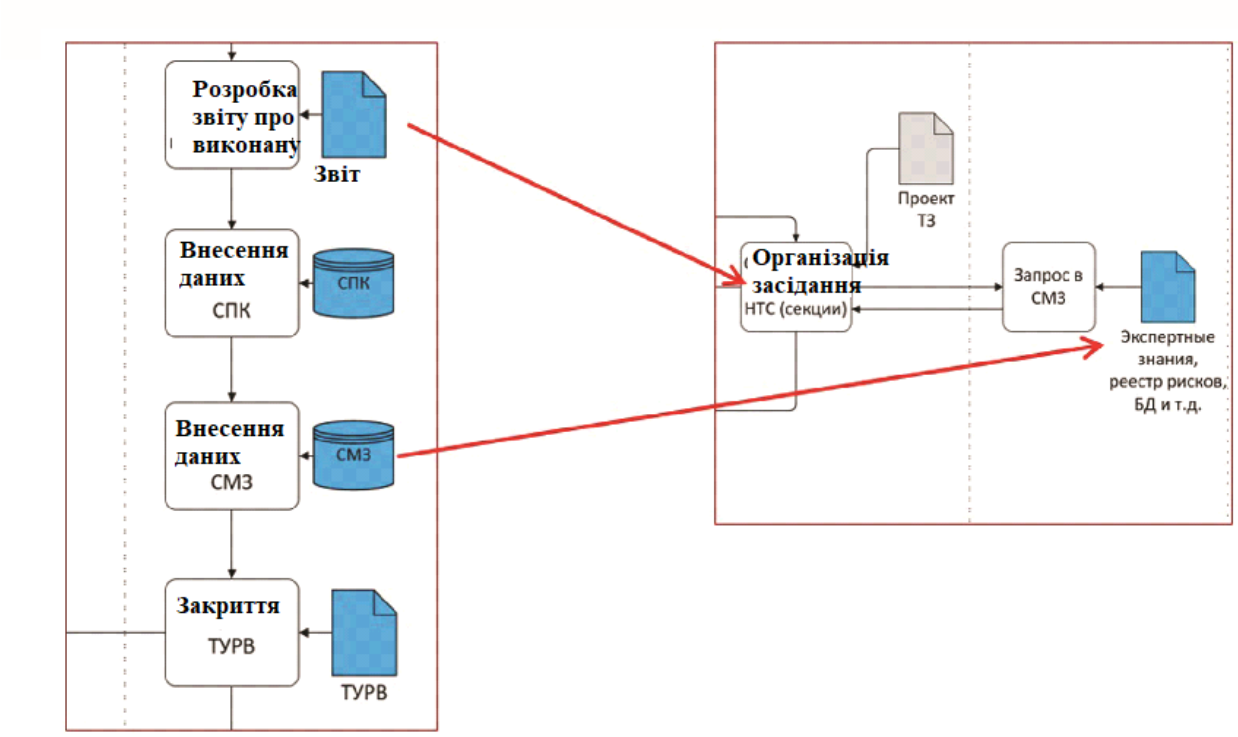

Рисунок 3.4. Системи застосування знанням при керуванні захистом інформації

Висновки до третього розділу

1. Одним з основних складових ризик-менеджменту в системі захисту інформації фармацевтичних підприємств є створення авторизованої імітаційної моделі кібератак на інформаційні системи, *бізнес – процеси*, *мобільні, веб і дескотопні додатки*, та їхню *бізнес – логіку*, а також на *персонал*.
2. Метою створення такої імітаційної моделі є пошук вразливості та проведення аналізу існуючих технічних каналів на їх захищеність, стійкість *бізнес – процесів* та персоналу підприємства до віддалених кібеатак.

3.Як результат проведення такого моделювання є багаторівневий звіт з аналізом захищеності фармацевтичного підприємства відповідно до кіберризиків та створення рекомендацій щодо усунення загроз та вразливостей.

4.Також таке імітаційне моделювання допомагає підприємству створювати безпечні системи інформаційного захисту та відповідні продукти щодо захисту інформації, даючи змогу мінімізувати фінансові та ресурсні втрати в разі кібератаки.

ВИСНОВКИ

1. В роботі було встановлено, що розробка безпечного програмного забезпечення не є загальноприйнятою практикою. Зазвичай головним пріоритетом для бізнесу при створенні коду є швидкість розробки, зручний інтерфейс та стабілинй та якісний робочий функціонал. Такий підхід призводить до того, що вісімдесят два відсотки усіх вразливостей системи інформаційного захисту знаходяться в самому програмному забезпеченні.
2. Було встановлено, що середня вартість кібератаки на мережеву інфраструктуру підприємства становить двісті тисяч доларів США, але всього чотирнадцять відсотків підприємств впровадили інструменти та процедури інформаційного захисту для створення власної системи кібербезпеки та захисту інформації.
3. З огляду на частоту кібер інцидентів, а саме кожні тридцять дев`ять секунд по всьому світу, варто регулярно перевіряти й оновлювати систему інформаційного захисту та кібербезпеки в цілому. Це є головною метою тестування на проникнення в корпоративну мережу.
4. У команди *етичних хакерів* 10*Guards* великий досвід у тестуванні системи безпеки мережі. Потрібно постійно проводити якісну оцінку стійкості *IT – середовища* з подальшим виявленням мережевих вразливостей, таких як: наявність шкідливого програмного забезпечення, неякісний контроль інформаційної безпеки та захисту інформації, недоліки програмного забезпечення, небезпечний брандмауер, маршрутизатор, користувацькі правила, небезпечні параметри конфігурації, непропатчені системи.
5. Було встановлено, що існує внутрішнє тестування на проникнення в мережу, яке здійснюється всередині та призначене для виявлення загроз, причиною яких є користувач або саме програмне забезпечення.
6. Також встановлено, що існує і зовнішнє тестування, яке призначене для оцінки засобів контролю інформаційної безпеки та захисту інформації периметру мережі та моделювання кібератак ззовні, а саме *веб*, *пошта*, *FTP – сервери*.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 1. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.

2. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.

3. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.

4. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.

5. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.

6. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.

7. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

8. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

9. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.

10. Агафьин С. С. LW-КРИПТОГРАФИЯ: ШИФРЫ ДЛЯ RFID-СИСТЕМ / С. С. Агафьин // Безопасность информационных технологий / С. С. Агафьин., 2011. – С. 30–33.

11. Гнатюк М. А. ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНОЙ ВОЛНЫ НА КАСКАДНОМ СОЕДИНЕНИИ ПРЯМОУГОЛЬНЫХ ВОЛНОВОДОВ / М. А. Гнатюк, В. М. Морозов, С. В. Марченко. // ХНУРЕ. – 2019. – №196. – С. 130–137.

12. Горбачов В. Е. ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ И ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ СИСТЕМ / В. Е. Горбачов, К. Б. Абдулрахман. // ХНУРЕ. – 2017. – №191. – С. 113–119.

13. Горбенко І. Д. ДОСЛІДЖЕННЯ СТРУКТУРИ СПЕКТРІВ СИГНАЛОВ З ЛІНІЙНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ / І. Д. Горбенко, О. А. Замула. // ХНУРЕ. – 2018. – №193. – С. 192–198.

14. Горбенко І. Д. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОМЕХОЗАЩИЩЕННОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ ВНУТРЕННИХ И ВНЕШНИХ ВОЗДЕЙСТВИИ / І. Д. Горбенко, А. А. Замула, В. Л. Морозов. // ХНУРЕ. – 2017. – №189. – С. 5–14.

15. Горбенко Ю. І. УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ [Електронний ресурс] / Ю. І. Горбенко, К. В. Ісірова // ХНУРЕ. – 2017. – Режим доступу до ресурсу: https://nure.ua/wp content/uploads/2017/Scientific_editions/191/5.pdf.

16. Описание процесса радиочастотной идентификации [Електронний ресурс] – Режим доступу до ресурсу: http://asupro.com/gps-gsm/meansidentification/reference/description-process-rfid.html.

17. Сальников Д. С. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН / Д. С. Сальников, А. І. Цопа. // ХНУРЕ. – 2018. – №192. – С. 140–148.

18. Шарфельд Т. Системы RFID низкой стоимости / Т. Шарфельд. – Москва, 2006. – 197 с.