ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Центр заочної та дистанційної освіти

Кафедра “Економіка, менеджмент та комерційна діяльність”

Допущена до захисту:
Завідувач кафедри економіки, менеджменту та комерційної діяльності к.е.н., доцент
_____ Тетяна РЯБОВОЛИК
“_03_” __січня_____ 2024 р.
(протокол засідання кафедри ЕМКД №10 від 03 січня 2024 р.)

.

Кваліфікаційна робота

за другим (магістерським) рівнем вищої освіти:

на тему: “Управління забезпеченням інформаційної безпеки підприємства”

Виконав: здобувач вищої освіти ІІ курсу магістратури, групи УФЕБ - 22 МЗ спеціальності 073 "Менеджмент" (ОПП Управління фінансово-економічною безпекою)
Гарань Денис Сергійович_____
Керівник: к.е.н., проф. кафедри ЕМКД
Левченко Анна Олександрівна_____
Рецензент: д.е.н., професор
Шалімова Наталія Станіславівна_____

м. Кропивницький – 2023

ЗМІСТ

ВСТУП 4
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 7
1.1. Поняття інформаційної безпеки, її роль та основні складові 7
1.2. Основні види загроз та методи забезпечення інформаційної безпеки 18
1.3. Специфіка організації інформаційної безпеки на підприємствах агропромислового комплексу 22
РОЗДІЛ 2. ОЦІНКА СТАНУ ЗАБЕПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРИКЛАДІ ТОВ «МХП-УРОЖАЙНА КРАЇНА» 33
2.1. Загальна характеристика діяльності ТОВ «МХП-Урожайна країна» 33
2.2. Аналіз основних економічних показників діяльності підприємства 42
2.3 Стан інформаційної безпеки на підприємстві ТОВ «МХП-Урожайна країна» 57
РОЗДІЛ 3. ПРОЕКТ ЗАХОДІВ ІЗ ЗАБЕПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ НА ПРИКЛАДІ ТОВ «МХП-УРОЖАЙНА КРАЇНА» 68
3.1 Методи забезпечення інформаційної безпеки агропромислових підприємств 68
3.2 Пропозиції щодо удосконалення основних напрямів підвищення ефективності роботи та інформаційної безпеки ТОВ «МХП-Урожайна країна» 76
ВИСНОВКИ 85
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 90
ДОДАТКИ 98

ВСТУП

Ефективне управління діяльністю підприємства може здійснюватися лише за умови формування його як системи, головним призначенням якої є вирішення основних завдань управління. Тому важливою умовою забезпечення можливостей до сталої діяльності та розвитку підприємств у наших економічних умовах є сформована система управління інформаційною безпекою. Цю систему слід розглядати як компіляцію спільних елементів, що одночасно відокремлені від середовища та взаємодіють із ним як спільне ціле. Структура управління інформаційною безпекою за різними рівнями забезпечує запобігання руйнівних впливів з боку різноманітних внутрішніх та зовнішніх факторів. При цьому вона захищає і саме середовище підприємства, за межами якого підприємство не може функціонувати без загрози стабільності його діяльності.

Забезпечення інформаційної безпеки сучасного агропромислового підприємства повинно захищати в першу чергу взаємодію всіх елементів, засобів та заходів системи безпеки. Це стає можливим лише за умови чітко побудованого механізму забезпечення безпеки підприємства, якому відводиться найважливіша роль в управлінні. Особливу роль в цьому разі надається проблемі розстановки пріоритетів та намічених напрямів розвитку підприємства. Стратегія внутрішньовиробничих процесів (політика управління оновленням основних засобів, технічне та технологічне переозброєння, впровадженню інновацій, систем мотивації та розвитку персоналу тощо) також потрапляє під захист системи забезпечення інформаційної безпеки..

Таким чином, забезпечення інформаційної безпеки підприємства, з одного боку, є складовою його інтересів, цілей та пріоритетів розвитку, та одночасно вимагає вивчення та розуміння стану зовнішнього та внутрішнього оточення для запобігання існуючим та потенційним загрозам.

Отже, можна вважати, що сучасними особливостями становлення

української економіки в об'єктивних умовах існуючих внутрішніх та зовнішніх загроз роблять проблему інформаційної безпеки надважливими. Рішення цієї проблеми стає одним із пріоритетних напрямків як державної соціально-економічної регіональної політики, так і умовою стабільного та захищеного існування регіонального рівня. Саме від рішення проблем безпеки на рівні окремого регіону, окремо взятого підприємства, залежить загальний стан економічної та інформаційної безпеки держави.

Інформація в сучасному світі є вкрай важливим ресурсом та інструментом. З її допомогою ведуться війни, проводяться виборчі компанії та укладаються багатомільйонні контракти. У нашому столітті інформаційних технологій інформація відіграє дуже важливу роль. Неправомірне використання, фальсифікація, будь-яке пошкодження або розголошення хоча б частини конфіденційної чи економічної інформації (так само як і дезорганізація процесів її обробки та передачі) в інформаційно-керуючих системах, завдасть значної шкоди (як матеріальної так і моральної) більшості суб'єктів, що беруть участь у виробничих процесах. Саме тому дуже важливо захищати її.

Захист інформації є прийняття правових, організаційних та технічних заходів, спрямованих на:

- убезпечення інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, розповсюдження, а також інших неправомірних дій щодо такої інформації;

- дотримання конфіденційності інформації обмеженого доступу;

- реалізацію права доступу до інформації».

Мета роботи є розробка зведеного комплексу рекомендацій щодо забезпечення інформаційної безпеки на підприємстві, на основі збору та аналізу заходів та засобів забезпечення інформаційної безпеки на великих та малих підприємствах.

Об'єкт дослідження – ТОВ "МХП-Урожайна країна".

Предмет дослідження – система управління інформаційною безпекою

підприємства.

Метою дослідження є розробка шляхів удосконалення системи управління інформаційною безпекою підприємства ТОВ «МХП-Урожайна країна». Ця мета визначила такі завдання:

– розглянути теоретичні аспекти формування системи управління інформаційною безпекою підприємства;

– надати загальну характеристику ТОВ «МХП-Урожайна країна»;

– проаналізувати основні показники фінансового становища ТОВ «МХП-Урожайна країна»;

- провести оцінку існуючої системи управління інформаційної безпеки підприємства;

- розробити заходи щодо вдосконалення формування системи управління інформаційною безпекою підприємства ТОВ «МХП - Урожайна країна».

В кваліфікаційній роботі використано наступні методи: монографічний, табличний, графічний, балансовий, розрахунково-конструктивний, порівняльний, методики оцінки фінансового стану підприємства та ефективності діяльності та інші.

Інформаційною основою дослідження виступили практичні матеріали та звітність ТОВ «МХП - Урожайна країна». Теоретичною основою дослідження стали праці українських та зарубіжних науковців у галузі інформації. економіки та фінансів, статті періодичного друку з питань інформаційної безпеки підприємства.

У якості апробації результатів кваліфікаційної роботи були опубліковані тези на тему «Основні види загроз та методи забезпечення інформаційної безпеки» у збірнику VI Міжнародної науково-практичної конференції «Конкурентоспроможна модель інноваційного розвитку економіки України», 7-8 грудня 2023 року.

Робота складається з вступу, трьох розділів, висновків, бібліографічного списку та додатків.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття інформаційної безпеки, її роль та основні складові

У сучасному світі, де інформаційні технології отримують все більш важливу роль у всіх сферах життєдіяльності людини (особливо у бізнесі), гарантія безпеки інформації стає критичною вимогою для сталого розвитку суспільства взагалі та його економічних складових зокрема. Загрози з боку кіберзлочинців, несанкціонований доступ до даних, виток інформації та інші ризики вимагають від компаній ефективного управління інформаційною безпекою. Розглянемо основні напрямки та особливості управління інформаційною безпекою на рівні підприємства, а також роль структур та політик інформаційної безпеки у забезпеченні захисту даних.

Основними напрямками керування інформаційною безпекою є:

1. систематична ідентифікація та аналіз вразливостей у своїх інформаційних системах та інфраструктурі. Це включає оцінку ризиків, пов'язаних із конфіденційністю, цілісністю та доступністю даних, а також визначення критичних активів та їх захищеності.

2. розробка та впровадження сталих систем інформаційної безпеки. Компанії повинні дотримуватися чіткої політики інформаційної безпеки, яка визначає правила та процедури для забезпечення захисту інформації. Це може включати вимоги щодо використання певних паролів, управління доступом, шифрування даних, резервного копіювання та інших аспектів інформаційної безпеки.

3. навчання співробітників є обов’язковим, адже співробітники є найбільш слабкою ланкою в структурі інформаційної безпеки, тому необхідно привчати їх до базових основ безпечної поведінки в інформаційному просторі. Навчання може включати інформування про

типові атаки, фішингові спроби, правила обробки конфіденційної інформації та регулярні тренінги з безпеки.

4 Захист від кібератак: компанії повинні застосовувати сучасні технічні засоби захисту, системи виявлення та попередження вторгнень та якісні антивірусні програми. Ці заходи допоможуть виявити та запобігти несанкціонованому доступу до важливої та інформації та відновлювати працездатність систем після інцидентів.

5 Керування доступом до інформації є важливою складовою управління інформаційною безпекою. Організації повинні встановити надійні системи автентифікації, авторизації та обліку, що гарантують, що лише авторизовані співробітники отримують доступ до важливих даних [1].

Визначити, наскільки вразлива система, можна за її слабкою ланкою. Вважається, що цією ланкою є людина. Саме він — найімовірніше джерело загроз інформаційній безпеці. Будь-яка організація основні сили спрямовує рішення технологічних завдань, не надаючи особливого значення «людській» складовій. Однак можна скільки завгодно розвивати та вдосконалювати технічні засоби, але вони залишаються лише інструментом у вирішенні питань безпеки. Саме від людини залежить, наскільки ефективно буде здійснено безпекову політику. Не секрет, що зловмисники часто використовують не стільки вразливість технічних чи програмних засобів, скільки некомпетентність співробітників саме у питаннях дотримання безпеки та наявну відсутність контролю за дотриманням елементарних правил з боку керівництва на робочих місцях. Тому важливого значення для забезпечення загальної безпеки організації набуває кадрова безпека. Комплекс організаційних заходів з управління персоналом включає: грамотний підбір кадрів, навчання співробітників питанням інформаційної безпеки, мотивацію методами заохочення та за допомогою санкцій за скоєні порушення, а також контроль за дотриманням встановлених правил. Вирішення питань щодо реалізації цих заходів лягає на структуру, що забезпечує безпеку підприємства. Західні фахівці із забезпечення економічної

безпеки вважають, що збереження конфіденційної інформації на 80% залежить від правильного підбору, розміщення та виховання персоналу [3].

Робота з персоналом починається з підбору кадрів та прийому на роботу. Підбір кадрів передбачає ретельний відбір та попередню перевірку кандидатів. На цьому етапі доцільно проводити співбесіди, анкетування, спостереження, щоб отримати найповніше уявлення потенційного працівника, виявити його рівень інтелекту, скласти психологічний портрет, визначити моральні якості. При прийомі працювати важливо підписання працівником як трудового договору, куди входять у собі умова дотримуватися встановлених у організації правила безпеки, і зобов'язання про нерозголошення відомостей, складових комерційну таємницю, конфіденційної інформації, іншої важливої інформації, доступом до якої він отримає під час роботи. Також працівника має бути попереджено про відповідальність за недотримання встановлених правил і за розголошення зазначених відомостей. Важливим для перевірки нового працівника на відповідність займаній посаді є встановлення йому випробувального терміну, протягом якого він має проявити себе, довести, що здатний працювати з важливою, конфіденційною інформацією.

Для роботи з документами, що містять конфіденційні відомості, керівник організації надає працівникові дозвіл на доступ до таких відомостей. При цьому важливо розмежувати доступ до конфіденційних документів з тематики інформації та користувачів, яким ця інформація необхідна для роботи. Розмежування прав доступу дозволяє суворо обмежити склад персоналу, до обов'язків яких входить робота з конфіденційними документами, щоб унеможливити доступ до важливих відомостей сторонніх осіб.

Наступним важливим напрямом роботи з персоналом є його навчання з питань інформаційної безпеки. Навчання може бути первинним та повторним. Первинне навчання необхідно проводити для новоприйнятих співробітників, які мають освоїти основні способи та прийоми захисту

інформації, перш ніж розпочати виконання своїх посадових обов'язків. Подальше навчання проводиться підвищення професійної кваліфікації працюючих співробітників. Процес навчання повинен здійснюватися регулярно, а не час від часу. Звичайна періодичність навчання становить раз на 3-5 років. У виняткових випадках, пов'язаних із впровадженням на підприємстві нових автоматизованих інформаційних систем, зміною вимог політик безпеки, а також зміною основних бізнес-процесів, потрібне проведення з персоналом додаткових позапланових занять [45].

За підсумками навчання доцільно перевірити, наскільки співробітники засвоїли знання. Це може бути у формі тестування чи вирішення конкретної задачі. Персонал, який не пройшов цієї перевірки, має бути усунений від роботи з конфіденційною інформацією.

Одночасно з навчанням необхідно проводити інструктажі, на яких працівники служби безпеки доводять до відома працівників важливу інформацію - це вказівки керівництва щодо захисту інформації, відомості про факти виникнення загроз витоку інформації, у тому числі з вини працівників, про вжиті додаткові заходи захисту. Інструктажі на відміну занять проводяться не регулярно, а при необхідності.

Поряд з навчанням та інструктажем важливо здійснювати повсякденну роботу з персоналом, постійно нагадувати співробітникам про необхідність бути обережними. Дієвим заходом управління персоналом є мотивація, яка може бути реалізована як шляхом застосування заохочень, так за допомогою санкцій. Заохочення — це грошові виплати (премії, надбавки до заробітної плати), які застосовуються до працівників, які особливо відзначилися у роботі щодо зміцнення інформаційної безпеки. Підлягають заохочення працівники, які сприяли виявленню джерел витоку інформації, які розробили нові способи та засоби захисту цієї інформації. Крім матеріальних методів заохочення доцільно застосовувати та нематеріальні, такі як підвищення по службі, публічне визнання досягнень співробітника.

Однією з важливих складових мотивації персоналу є створення

сприятливого психологічного клімату на підприємстві, при якому застосовувані обмежувальні заходи або додаткові обов'язки будуть сприйматися співробітниками спокійно, з розумінням важливості для спільної справи щодо забезпечення інформаційної безпеки. Санкції застосовуються до співробітників, які допустили недбалість, грубе порушення встановлених правил, що призвело до витоку важливої інформації або створило загрозу інформаційній безпеці підприємства в цілому. Санкції, реальна можливість їх застосування, мотивують співробітників на дисциплінованість, дотримання регламенту захисту конфіденційної інформації, виконання всіх встановлених вимог. Застосовують формальні та неформальні санкції [37].

Формальні санкції — це передбачені законом заходи покарання, які застосовуються до порушників виходячи з наказів, рішень. До таких санкцій належать: усунення від роботи з конфіденційною інформацією шляхом переведення співробітника на інше робоче місце, позбавлення премій, відмова у продовженні строкового трудового договору, звільнення з роботи. Неформальні санкції припускають психологічний вплив на працівника. Це може бути аналіз допущеного порушення як під час індивідуальної бесіди з керівником підприємства, так і колективне обговорення на нараді. Неформальні санкції часто ефективніші, оскільки засудження своїх колег переживається важче, ніж наказ із доганою. Контроль за дотриманням встановлених правил захисту інформації також належить до комплексу заходів з управління персоналом.

Контроль здійснюється безперервно силами працівників служби безпеки підприємства. І тому використовуються організаційні, технічні заходи, і навіть робота з довіреними особами (інформаторами, співробітниками детективних агентств). Контроль може проводитись у формі планових та раптових перевірок на предмет дотримання працівниками правил роботи з конфіденційною інформацією та визначення справності та працездатності технічних засобів захисту; постійного моніторингу ситуації за

допомогою позаштатних інформаторів служби безпеки та з використанням спеціальних технічних засобів (наприклад, деталізація дзвінків службовими телефонами, спостереження за персоналом за допомогою камер відеоспостереження, аналіз інтернету, електронної пошти для вивчення зв'язків співробітників). Підлягає контролю також лояльність персоналу, тобто вірність його організації. Контроль лояльності працівників, які мають доступ до особливо конфіденційної інформації, здійснюється у постійному режимі.

Впровадження заходів інформаційної безпеки повинно забезпечити захисти інформації та усієї інформаційної інфраструктури підприємства від зовнішніх та внутрішніх негативних впливів. Результат таких впливів може привести як до втрати важливої інформації, так і до її несанкціонованої зміни чи, навіть, витоку за межі підприємства та її використання третіми особами. Саме тому інформаційна безпека стає важливим аспектом захисту бізнесу та забезпечення його сталості.

Принципами ефективного використання на підприємстві різноманітних систем інформаційної безпеки є:

1. Конфіденційність - організація та підтримка ефективного контролю та забезпечення достатнього рівня безпеки даних на різних етапах бізнес-процесів. Підтримка конфіденційності обов'язково застосовується при збереженні та транзиті інформації у будь-якому форматі.

2. Цілісність – структурування елементів управління, що забезпечують як внутрішню так і зовнішню послідовність доступу до інформації. Забезпечення її дозволяє запобігати спотворенню даних на будь-якому з етапів ділових операцій.

3. Доступність забезпечує повноцінний доступ до джерел інформації для тих посадових осіб, які мають певні повноваження. Головним завданням тут є передбачуваність процесів, що відбуваються у середовищі. Тоді користувачі мережі матимуть можливість доступу до усіх необхідних даних у будь-який час. Одним із головних факторів доступності інформації є

можливість відновлення системи після збоїв . Такий фактор проілюструвала хакерська атака на мережу «Київстар», що відбулася в грудні 2023 року. Завдяки доступності до джерел інформації відповідних осіб фактично зруйновану структуру компанії вдалося відновити в короткі строки. Чим мінімізували негативний вплив на функціонування компанії [10].

Забезпечення повноцінної та надійної інформаційної безпеки підприємства можливе лише за умови застосування комплексного та системного підходу до усієї проблеми безпеки. Система інформаційної безпеки будується з урахуванням усіх діючих та передбачених загроз та вразливостей. Тому важливим завданням для існування підприємства стає рішення проблеми забезпечення підтримки безперервного контролю, який має діяти щодня та цілодобово. Важливою умовою також стає забезпечення абсолютного контролю на всіх етапах життєвого циклу інформації, починаючи з моменту її надходження до компанії та закінчуючи втратою її актуальності чи знищенням.

Існує декілька видів контролю, що забезпечують загальний контроль за інформаційною безпекою. Їх впровадження дозволить компанії знижувати ризики у цій сфері та підтримувати їх на прийнятному рівні. Розрізняють:

• Адміністративний контроль.

Адміністративний контроль інформаційної безпеки – цілісна система, яка складається з мережі стандартів, принципів та процедур, що існують на підприємстві. Цей вид контролю створює та забезпечує певні кордони для ведення бізнес-процесів та управління персоналом. Він складається з законодавчих та нормативних актів, базується на прийнятій на підприємстві політиці корпоративної безпеки, контролює систему найму нових співробітників, здійснює дисциплінарне та інше втручання в життєдіяльність підприємства.

• Логічний контроль.

Структура логічного контролю передбачає використання усіх доступних засобів управління (засобів технічних), які працюють на захист

інформаційної системи від небажаного доступу. До цих засобів включають спеціальне програмне забезпечення, брандмауери, паролі тощо.

• Фізичний контроль.

Фізичний контроль використовується на робочих місцях та засобах обчислення. Він передбачає ефективне функціонування інженерних систем підприємства, порушення в роботі яких вплине на зберігання та передачу інформації. Такими системами вважаються опалення та кондиціювання, протипожежні системи. Другою важливою частиною фізичного контролю є системи управління доступом на об'єкти підприємства [23].

Інформаційна інфраструктура підприємства постійно наражається на численні загрози, які за своїм походженням діляться на кілька видів:

• Природні загрози, що виникають від обставин, які не залежать від людини. Це фарс-мажори на кшталт ураганів, пожеж, ударів блискавки, повеней та інших природних катаклізмів.

• Штучні загрози інформаційної безпеки виникають виключно завдяки людині. Під штучними загрозами розуміють навмисні та ненавмисні. Навмисними вважають дії конкурентів, хакерські атаки, шкідництво скривджених працівників і т. д. Ненавмисними загрозами вважають ті, що виникли внаслідок дій, вчинених через недостатність компетентності або з необережності.

• Внутрішні загрози - виникають усередині інформаційної інфраструктури підприємства.

• Зовнішні загрози – створюються за межами інформаційної інфраструктури підприємства [26].

Залежно від характеру впливу загрози інформаційній безпеці поділяються на пасивні та активні. Пасивні загрози — це чинники впливу, які можуть змінювати зміст і структуру інформації. Активні загрози можуть вносити шкідливі зміни. До них відносять, наприклад, вплив шкідливого програмного забезпечення.

Головну загрозу становлять штучні навмисні небезпеки. Враховуючи

на зростання комп'ютеризації у різноманітних сферах бізнесу та збільшення кількості електронних транзакцій, ці загрози швидко розвиваються. Пошуки способів отримання потрібної зловмисникам інформації та заподіяння шкоди компаніям, призводять до активного використання сучасні технологій та програмних рішень. Їхні дії призводять до значних збитків, як у вигляді прямих фінансових втрат так і у вигляді втрати інтелектуальних здобутків. Саме тому інформаційна безпека підприємства має використовувати новітні технології з обов’язковим залученням актуальних засобів захисту даних.

Засобами захисту інформації вважаються пристрої, організаційні заходи, прилади, програмне забезпечення що має на меті запобігати витокам інформації та забезпечує її збереження при загрозі зовнішнього негативного впливу.

В залежності від способів реалізації, розрізняються і засоби захисту інформаційної безпеки. Вони бувають наступних типів:

- Організаційні засоби - комплекс заходів організаційно-правового та організаційно-технічного характеру. Це - законодавчі та нормативні акти, внутрішні нормативні документи організації. Другий тип - заходи що забезпечують обслуговування інформаційної інфраструктури підприємства.
- Апаратні або технічні засоби - спеціальне обладнання та пристрої, що запобігають витоку, та захищають від проникнення в інфраструктуру.
- Програмні засоби - спеціалізоване програмне забезпечення, яке захищає, контролює та зберігає інформації.
- Програмно-апаратні засоби - спеціальне обладнання для використання програмного забезпечення захисту даних [69].

Найбільшого поширення сьогодні набули програмні засоби захисту інформації. Вони повністю відповідають вимогам ефективності та актуальності, регулярно оновлюються, ефективно реагуючи на актуальні загрози штучного характеру.

Для захисту даних у сучасних мережах використовується широкий спектр спеціалізованого програмного забезпечення. Можна виділити

наступні типи програмних для захисту інформації:

• Антивірусне програмне забезпечення - спеціальні програми для боротьби та видалення комп'ютерних вірусів. Вони діють як під час позапланових перевірок, так і за раніше налаштованим. Ці програми аналізують діяльність інфраструктури та виявляють чи блокують підозрілу активність інших програм. Сучасні антивіруси здатні навіть відновлювати файли, які раніше були заражені шкідливими програмами.

• Хмарні антивіруси - сервіси Crowdstrike, Panda Cloud Antivirus, Immunet та багато інших. Їх основний функціонал програмного забезпечення розміщений у хмарі, а на персональному комп'ютері, що знаходиться під їх захистом, встановлений «клієнт» - програма з невеликими технічними вимогами. Вона потрібна для вивантаження у хмарний сервер основної частину для аналізу. Це забезпечує ефективний антивірусний захист не вимагаючи великих ресурсів від обладнання.

• Рішення DLP (Data Leak Prevention) – це спеціальні програмні рішення, що блокують спроби несанкціонованого витоку даних. Це комплекс програм, які захищають підприємства від втрати інформації з різних причин.
• Системи криптографії (наприклад DES - Data Encryption Standard, чи AES - Advanced Encryption Standard). Ці програми перетворюють потрібні дані в шифровані масиви. Для їх розшифровки потрібно використовувати відповідні шифри. Також криптографія здатна використовувати інші корисні програми для захисту інформації. Сьогодні нові програми, які використовують шифровані комунікації, наприклад Secure Shell (SSH), витісняють застарілі рішення через їх не здатність забезпечувати необхідний рівень безпеки. Такі програми як Telnet і протокол передачі файлів FTP.

• Міжмережеві екрани (МСЕ) – це рішення, що забезпечують надійну фільтрацію та блокування неконтрольованого трафіку, відстежуючи доступ до мережі. Міжмережевий екран зазвичай зроблений у форматі програми, яка встановлюється на звичайний комп'ютер. Програмно-апаратний фаєрвол - це спеціальний пристрій на базі операційної системи з встановленим

міжмережевим екраном. Крім основних функцій, вони здатні запропонувати низку додаткових рішень для внутрішніх мереж. Наприклад, виступають як сервер VPN.

• Віртуальні приватні мережі VPN (Virtual Private Network). Рішення, що використовує в межах загальнодоступної мережі приватну мережу для передачі та прийому даних, що дає ефективний захист підключених до мережі програм. За допомогою VPN забезпечується можливість віддаленого підключення до локальної мережі, створення спільної мережі головного офісу з філіями. Безпосередньо для користувачів VPN дає можливість приховувати розташування та захист дій, що виконуються в мережі.

• Проксі-сервер – програма, яка виконує функцію розподілу між комп'ютером та зовнішнім сервером. Запит, від користувача на сервер, спочатку надходить на проміжну ланку і вже від імені цієї ланки надходить на сервер. Зворотна передача інформації відбувається за тією ж схемою.

• Рішення SIEM – системи моніторингу та управління інформаційною безпекою. Спеціалізоване програмне забезпечення, що перебирає на себе функцію управління безпекою даних. Це забезпечується збиранням відомостей про події з усіх функціоналів, які підтримують безпеку. А також від операційних систем. Така система аналізує зібрані дані та забезпечує їх централізоване зберігання в журналі подій. На підставі повного аналізу даних система здатна виявити можливі збої, атаки хакерів,чи інші відхилення та можливі інформаційні загрози [79].

Враховуючи широке використання мобільних пристроїв для передачі даних співробітниками компанії, у системі інформаційної безпеки обов'язково має бути врахований і цей фактор. З метою контролю передачі інформації через мобільні пристрої для захисту цієї інформації потрібно застосовувати такі програмні продукти як Blackberry Enterprise Mobility Suite, IBM MaaS360, VMware AirWatch та інші [74].

Забезпечення інформаційної безпеки сьогодні є нагальна потреба, зневага якої може мати руйнівні наслідки для бізнесу. Широкий набір засобів

та рішень, доступних сьогодні захисту інформації, може ускладнювати вибір для підприємства. Забезпечити безпеку IT-інфраструктури дозволяє певний набір інструментів, який необхідно підбирати індивідуально. Це дозволить реалізувати багаторівневу систему захисту, яка забезпечить надійну нейтралізацію актуальних загроз.

Видбір необхідних інструментів для захисту інформації за умови створення системи повинен здійснюватися з врахуванням певних факторів, до яких відносяться:

- напрямки професійної та виробничої діяльності компанії;
- масштабність виробництва, з урахуванням усіх територіально віддалених підрозділів, та тих структурних підрозділів, що вимагають особливого IT-захисту;
- технічне забезпечення підприємства;
- стан професійної та безпекової підготовки персоналу, зайнятого в системі інформаційного забезпечення діяльності підприємства.

Існуючий на підприємстві IT-підрозділ зазвичай не здатний реалізувати такий комплексний підхід через інші цілі та завдання, що постають перед ним. Завдяки цьому виникають великі прогалини у захисті, що стає загрозою втрати чи пошкодження цінної інформації внаслідок несанкціонованого втручання ззовні.

Тому розробку та впровадження системи забезпечення безпеки інформації на підприємстві мають проводити професіонали.

1.2. Основні види загроз та методи забезпечення інформаційної безпеки

Загрози інформаційної безпеки діляться на два види: природні та штучні. Природними вважаються ті явища, що повністю не залежить від людини, наприклад урагани та інші стихійні лиха. Штучним загрозами вважаються ті. що залежать безпосередньо від людини. В свою чергу вони

розподіляються на навмисні та ненавмисні. Ненавмисні виникають через необережність чи неуважність. Наприклад: встановлення сторонніх програм, що порушують роботу системи, та можуть призвести до втрати інформації. Навмисними загрозами вважаються ті, що створюються спеціально. До них можна зарахувати зовнішні атаки зловмисників, та внутрішні негаразди системи захисту компанії. Результатами цього виду загроз є можливість матеріальних чи інтелектуальних втрат для організації.

Основними джерелами загроз є як окремі зловмисники («хакери»), так і групи та державні спецслужби (кіберпідрозділи), що здатні застосовувати увесь арсенал доступних спеціалізованих засобів комп'ютерного злому. Щоб отримати доступ до потрібної інформації, вони здатні використовувати слабкі місця та помилки в роботі програмного забезпечення, що використовується в організації проти якої спрямовані злочинні дії [12].

Оцінка загроз інформаційній безпеці проводиться комплексно. Для кожного випадку обираються власні методи оцінки. Для унеможливлення втрати даних через несправне устаткування, необхідно використовувати тільки високоякісні комплектуючі, та використовувати своєчасне якісне та відповідне технічне обслуговування. Слід встановлювати та регулярно оновлювати програмне забезпечення у всій мережі підприємства. Окрема увага приділяється програмному забезпеченню, що виконує захисні функції: антівирус, анти спам та ін. Інформаційні бази таких програм повинні оновлюватися щодня.

Навчання працівників підприємства основам інформаційної безпеки та принципам роботи різноманітних загрозливих програм забезпечить комп'ютерну грамотність та зменшить ризик випадкових витоків даних. Як засіб запобігання втрати інформації слід планомірно та в обов'язковому порядку розробити систему створення резервних копій.

Якщо погрози спрямовані на злам програмних комплексів, які ви використовуєте, найчастіше на рівні користувача ви не зможете на це вплинути. Єдиний спосіб – не використовувати деякі програми.

Використовувати їх можна, якщо проникнення зловмисника не загрожує витіканням важливої інформації і не спричинить суттєвих втрат для вас.

Безпека від загроз, спрямованих на апаратуру, інфраструктуру або від загроз природного характеру, забезпечує хостинг-компанія, яку ви вибрали в якості орендодавця серверів. Підходьте до вибору хостинг-компанії уважно та відповідально, вона має на високому рівні забезпечити надійність апаратної та інфраструктурної складової.

До основних видів загроз інформаційній безпеці відносяться:

- внутрішні збої чи відмова інформаційної системи;
- відмова підтримуючої інфраструктури.

До основних загроз у підтримуючій інфраструктурі відносяться:

- збій у роботі, пов'язаний з навмисним або випадковим виходом з ладу електричних систем, систем зв'язку, водопостачання, теплопостачання та кондиціювання;
- обвал, руйнування чи пошкодження будівель та споруд;
- невиконання обслуговуючим персоналом своїх посадових обов'язків, зумовлене страйками, збоями у роботі транспортних служб, аваріями, природними катаклізмами, терористичними актами тощо [65].

Загрози цілісності поділяють на загрози статичної та динамічної цілісності, а також загрози цілісності службової інформації та змістовних даних.

Службовою інформацією є паролі для доступу, маршрути передачі даних у локальній мережі та інша подібна інформація. Дуже часто протиправні дії та хакерські атаки здійснює особа, яка є співробітником компанії, яка володіє необхідним обсягом інформації про режим роботи та заходи захисту.

Одна з загроз, від яких дуже важко знайти ефективний спосіб захисту – зловживання службовими повноваженнями. У багатьох системах передбачено надання доступу привілейованому користувачеві, яким може бути системний адміністратор, до всіх файлів та пошти будь-якого

користувача.

Також збитки можуть бути завдані при сервісному обслуговуванні, тому що сервісний інженер отримує необмежений доступ і має можливість в обхід захисних бар'єрів підібратися до будь-якого файлу.

Розрізняють такі способи, що забезпечують безпеку даних в інформаційних системах:

Перешкода – фізична перешкода, яка перешкоджає доступу зловмисників до секретної інформації. Наприклад, вхід до будівлі, де знаходиться сервер, що зберігає важливу інформацію, дозволено лише співробітникам компанії.

Управління доступом – доступ до інформації та її використання контролюється системою ідентифікації користувачів з перевіркою їх повноважень. Наприклад, секретна інформація зберігається в комп'ютерах, що знаходяться в приміщенні або на поверсі, доступ на який є тільки у співробітників, які мають спеціальні пропуски або мають логін і пароль для доступу до бази даних. Причому рівень наданих кожному співробітнику привілеїв може бути різним, залежно від рівня посади і виконуваного співробітником функціоналу.

Криптографія – один із способів збереження конфіденційності інформації та цілісності даних за допомогою шифрування шляхом перетворення тексту на спеціальний алгоритм. Яскравим прикладом є електронно-цифрові підписи чи зберігання інформації у блокчейні.

Захист від атак вірусних та шкідливих програм (віруси, трояни, мережеві черв'яки, логічні бомби) – використання антивірусних програм, зовнішніх накопичувачів інформації, резервне копіювання даних.

Регламентація – це спосіб інформаційного захисту, який допомагає практично виключити для зловмисника отримання доступу до конфіденційної інформації, що зберігається. Наприклад, багато компаній вводять заборону використання співробітниками особистих флешок, стверджують спеціальні правила і стандарти роботи, що регламентують

терміни створення резервних копій даних тощо.

Примус – встановлення певних правил під час роботи з програмами, які містять секретну інформацію, порушення яких тягне у себе матеріальну, адміністративну, а деяких випадках і кримінальну відповідальність.

Заохочування – заклик до співробітників про дотримання порядку по роботі з конфіденційною інформацією, щоб уникнути порушень морально-етичних норм, що склалися [66].

Розрізняють такі види засобів захисту:

Технічні засоби. Наприклад, встановлення сигналізації, захисних віконних решіток, використання пристроїв, що створюють перешкоди при спробі передачі даних по радіоканалах, спеціальні електронні перепустки у вигляді ключ-карт для входу в будівлі.

Програми для кодування та шифрування даних, антивірусні програми, бекап-системи, системи ідентифікації користувачів.

Змішані засоби. Комбінований комплекс технічних та програмних засобів, що забезпечують захист інформації.

Організаційні засоби. Законодавчі акти, нормативні документи, спеціалізовані правила, що регламентують діяльність у сфері захисту інформації, оснащення та відповідну підготовку приміщень з комп'ютерною технікою, проведення мережевих кабелів з урахуванням вимог щодо інформаційної безпеки та організація інших дій, що сприяють обмеженню доступу до баз даних.

1.3. Специфіка організації інформаційної безпеки на підприємствах агропромислового комплексу

Необхідність забезпечення інформаційної безпеки держави та підприємств в цілому продиктована умовами сучасної ринкової економіки. Інформаційна безпека важлива як для національної економіки, так і для її складових і ланок в цілому, включаючи окремі галузі та підприємства.

Зокрема, особливу роль відіграє інформаційна безпека підприємств таких важливих галузей національної економіки України, як агропромисловий комплекс.

Традиційні методи захисту інформації не завжди дозволяють підтримувати необхідний рівень інформаційної безпеки, що може мати негативний вплив на економічний стан підприємств, галузей та країни в цілому.

З початку 1990-х років нормативне регулювання процесів забезпечення інформаційної безпеки має досить значне змістовне наповнення.

На сьогоднішній день Україна (і майже всі країни після розпаду Радянського Союзу) має необхідну правову базу, і бізнес-організації можуть здійснювати діяльність із захисту інформації відповідно до існуючих нормативних актів. Однак повністю вирішити проблему інформаційної безпеки поки що зарано.

Стрімкий розвиток науково-технічних знань, широкий доступ до засобів розробки комп'ютерного програмного та апаратного забезпечення та їх потенційних застосувань підвищують вразливість підприємств до різноманітних загроз. Основною причиною такої вразливості є неточності та недоліки в існуючих політиках інформаційної безпеки підприємств. Прикладами таких неточностей є відсутність комплексного забезпечення інформаційної безпеки організації на різних рівнях, включаючи задачі обробки даних та не охоплення всього життєвого циклу інформації [11].

Порушення режиму безпеки комп'ютерної мережі компанії може скомпрометувати її великі електронні бази даних, що призведе до крадіжки, спотворення або знищення стратегічно важливої інформації. З огляду на вищесказане, забезпечення належного рівня інформаційної безпеки на підприємствах є одним з найсерйозніших питань. Така ситуація робить цю проблему важливою, сприяючи розвитку різних методологій створення систем забезпечення інформаційної безпеки на підприємствах.

Таким чином виникає необхідність розробки систем і політик які забезпечують інформаційну безпеку на підприємствах.

Інформаційна безпека стає однією з головних тем для наукових досліджень у всьому світі. В Україні питаннями інформаційної безпеки на державному рівні займається Державна служба спеціального зв'язку та захисту інформації України [4]. Ця стуктура займається стандартизацією та сертифікацією у сфері інформаційної безпеки.

За результатами досліджень [46] робиться висновок про загальний стан інформаційної безпеки на підприємствах агропромислового комплексу:

- Основними шляхами витоку інформації є власні працівники підприємства та спільні бізнес-партнери;

- В організаціях відсутній належний контроль за зберіганням, знищенням та копіюванням документів;

- Документи, що містять комерційну таємницю, часто не позначаються як такі;

- Недостатньо уваги приділяється захисту інформації в комп'ютерній мережі та засобах зв'язку компанії

- Компанії не усвідомлюють співвідношення між витратами на інформаційну безпеку та збитками, завданими захищеній інформації.

Важливим питанням інформаційної безпеки є кількісна оцінка. Існуючі методи та показники оцінки аспектів безпеки інформаційних систем, таких як робочі місця та корпоративні мережі, не дають точної оцінки інформаційної безпеки всього підприємства.

Іншою серйозною проблемою є відсутність універсальних та ефективних методів впровадження інформаційної безпеки для різних типів організацій.

Великі підприємства агропромислового комплексу, як комерційні, так і державні, мають великий досвід забезпечення інформаційної безпеки в умовах обмежених ресурсів. У більшості випадків служби безпеки та охорони займаються цими питаннями окремо.

Однак для малих та середніх підприємств (МСП) такий підхід неможливий через їхні розміри та витрати. Керівництво таких підприємств вважає за краще економити на заходах інформаційної безпеки, що може призвести до значних фінансових і моральних втрат і навіть руйнування бізнесу.

У процесі забезпечення корпоративної інформаційної безпеки доцільно виділити кілька послідовних етапів [32].

Перший етап - ідентифікація інформації та даних, що становлять комерційну таємницю. Це один з найважливіших елементів у системі заходів захисту інформації. Якщо визначення того, що підлягає захисту, є передчасним або неточним, ефективність системи захисту значно знижується або стає марною.

Другий етап - визначення потенційних шляхів витоку інформації. У багатьох випадках це може бути людський фактор, спільна діяльність з іншими суб'єктами, промислове шпигунство, недобросовісна конкуренція та використання технічних засобів для несанкціонованого доступу до інформації.

Третім етапом є вжиття заходів для захисту інформації. Сюди входить створення правової бази захисту інформації, організаційної системи захисту та системи технічного захисту.

Інформаційне забезпечення є основою всієї діяльності підприємства. Для його безпечного і нормального функціонування необхідно вживати якісних заходів, спрямованих на інформаційну безпеку. Інформація, в тому числі комерційна і виробнича, є одним з найважливіших факторів вирішення проблем і труднощів підприємств і відіграє найважливішу роль у забезпеченні економічної безпеки підприємств, що вимагає постійної уваги з боку керівництва підприємства.

З огляду на вищезазначене, розробка та вдосконалення інструментарію та методичного інструментарію оцінки інформаційної безпеки та впровадження заходів інформаційної безпеки на підприємствах

агропромислового комплексу є актуальним питанням.

Економічна безпека сільського господарства багато в чому залежить від фінансово-економічного становища в країні. В даний час близько 30% господарств в сільськогосподарському секторі економіки економічно нестабільні. Не дивно, що вивченню економічної безпеки в цій області присвячено значну кількість наукових робіт. Слід зазначити, що в даний час в науковому світі не існує спільного підходу до інтерпретації концепції економічної безпеки як диференціатора, так і підходу до її структурної організації, який є важливим елементом економічної безпеки, і умовою її розвитку.

Але більшістю вчених визнається екологічна безпека, як важлива складова інформаційної безпеки та ризиків, з нею пов'язаних. Мається на увазі стан навколишнього середовища, при якому ймовірність нанесення шкоди людині, природі і матеріальним ресурсам зводиться до мінімуму. Надмірне внесення мінеральних добрив і засобів захисту рослин призводить до зниження якості продукції і забруднення навколишнього середовища. Для підтримки рівня екологічної безпеки важливо впровадити механізми, які допоможуть запобігти виникненню негативних процесів в навколишньому середовищі і забезпечать виконання заходів з урахуванням дотримання екологічних принципів. Головну роль в забезпеченні економічної безпеки відіграють техніко-технічні елементи, що складаються з рівня впровадження технологій, відповідних кращим світовим аналогам на російських підприємствах агропромислового комплексу. Загрози включають зниження рівня технічного потенціалу підприємства, порушення технічної дисципліни і моральне старіння використовуваного обладнання і технологій. Зовнішнім фактором є зменшення доступності коштів на оновлення парку машин і тракторів. Все це призводить до фізичного і морального зносу обладнання, використання технологій і в цілому до зниження рівня технічної і технічної безпеки [74]. Провідну роль в забезпеченні безпеки відіграє ринкова економіка, яка характеризує внутрішні і зовнішні можливості, створювані

ринковим середовищем. Це захист від неправильної поведінки на ринку, недоліків у політиці компанії щодо продуктів та продажів, низької конкурентоспроможності та неправильного вибору стратегії ціноутворення. Першим сигналом зниження рівня ринкової безпеки є зниження частки, яку займають компанії, нездатність протистояти конкурентному тиску [49]. Ринкова безпека відображає рівень відповідності внутрішніх виробничих потужностей підприємства зовнішнім потребам, встановленим ринком. Основне завдання політики компанії-розробити стратегію і організувати процес доставки продукції споживачам. Правова безпека відіграє особливу роль у формуванні економічної безпеки бізнесу. Адекватний рівень правової безпеки підприємства визначає стан захисту економічних інтересів від внутрішніх і зовнішніх загроз [50]. Внутрішні загрози правовій безпеці включають порушення внутрішніх правил розпорядку дня, що регулюють процеси внутрішньої взаємодії між командою і окремими співробітниками.

Зовнішні загрози виникають при взаємодії з регулюючими органами, постачальниками ресурсів, покупцями продукції або конкурентами. Регулювання служб безпеки та юридичних послуг має важливе значення для забезпечення комплексного підходу до формування правової безпеки сільськогосподарських підприємств. Їх можна комбінувати в контексті налаштування функціональності для підвищення ефективності вирішення проблем. Для малого бізнесу можна замовити послуги юридичної фірми з висококваліфікованими фахівцями з розробки та впровадження режиму правової безпеки, щоб виправдати дотримання превентивних заходів і високий рівень правової безпеки. Агропромисловий комплекс України значно впливає на економіку країни і її міжнародний статус в економічному плані, враховуючи його масштаби, з точки зору впливу і масштабів його впливу на економіку країни, є досить складною галуззю. В умовах російсько-української війни, сільськогосподарська продукція стала чи не єдиним важелем на зовнішньоекономічному ринку збуту.

Сучасна економіка закладає основи економічної безпеки

агропромислового комплексу з показниками стійкості розвитку агропромислового комплексу. Сама по собі економічна безпека агропромислового комплексу являє собою складну взаємодію економічної системи сільськогосподарського виробництва на всіх етапах виробництва і продажів для досягнення оптимального функціонування.

Відповідно до поширеної класифікації, загрози інформаційної безпеки ділять на навмисні та випадкові [23].

Загрози, не пов'язані з навмисними діями зловмисників та реалізуються у випадкові моменти часу, називаються ненавмисними чи випадковими. Реалізація таких загроз спричиняє найбільші втрати інформації. За даними NIST (National Institute of Standards and Technology – Національного інституту стандартів та технологій) близько 65% випадків порушення інформаційної безпеки викликається помилковими та неправильними діями користувачів та обслуговуючого персоналу [91].

Всі інші небезпеки, які не належать до першого класу, визначають як навмисні небезпеки. Цей клас вивчений недостатньо, досить динамічний і постійно доповнюється новими різновидами загроз.

Найпоширенішою загрозою такого класу є несанкціонований доступ до інформації.

Результати досліджень [46] дозволяють зробити висновки про стан інформаційної безпеки на підприємствах АПК:

- основними каналами витоку інформації є власні співробітники та партнери по спільному бізнесу;

- під час укладання договорів який завжди обмовляються заходи щодо інформаційної безпеки, відповідальність за розголошення інформації;

- відсутність на підприємствах контролю за зберіганням, знищенням та копіюванням документів;

- документи, що містять комерційну таємницю, часто не мають відповідного грифу;

- не приділяється достатньої уваги способам захисту інформації в

корпоративних комп'ютерних мережах підприємства та засобах зв'язку;

- підприємства не мають у своєму розпорядженні відомостей про співвідношення витрат на забезпечення інформаційної безпеки з втратою завданої інформації, що захищається.

Важливою проблемою інформаційної безпеки є її кількісна оцінка. Існуючі методики та показники оцінки елементів безпеки інформаційної системи, наприклад, робочого місця або корпоративної мережі, не дозволяють вірно оцінити інформаційну безпеку всього підприємства.

Ще однією важливою проблемою є відсутність універсальних дієвих методик реалізації інформаційної безпеки для підприємств різного типу. На великих підприємствах АПК, як комерційних, так і державних, є багатий досвід роботи із забезпечення інформаційної безпеки ресурсів обмеженого користування Найчастіше служби охорони та безпеки окремо займаються цими питаннями.

Але на підприємствах малого та середнього бізнесу такий підхід не можливий через його масштаби та вартість. Керівництво таких підприємств воліє заощаджувати на заходах інформаційної безпеки, що може призвести до значних фінансових та моральних втрат, аж до знищення підприємства.

У процесі забезпечення інформаційної безпеки підприємства варто виділити кілька послідовних стадій (рис.1.1).



Рис.1.1. Головні стадії інформаційної безпеки

Джерело:[складено автором]

Перша стадія - визначення відомостей, даних, що становлять комерційну таємницю. Це один із найважливіших елементів у системі заходів інформаційного захисту. Несвоєчасне чи неправильне визначення предмета захисту значно знижує ефективність системи захисту, або взагалі робить її марною.

Друга стадія – визначення можливих каналів витоку інформації. Найчастіше ними можуть бути: людський фактор, спільна діяльність з іншими суб'єктами, промисловий шпигунство, недобросовісна конкуренція, використання технічних засобів несанкціонованого доступу до інформації.

Третя стадія - вжиття заходів щодо захисту інформації. Сюди можна віднести створення: правових засад захисту інформації, організаційних систем захисту, технічні системи захисту [4].

Інформаційне забезпечення є основу будь-якого виду діяльності підприємства. Для нього безпечного нормального функціонування необхідно вживати якісних заходів інформаційної безпеки. Інформація, у тому числі комерційна, промислова, є одним із важливих факторів вирішення проблем та завдань підприємства, що виконує найважливішу роль у забезпеченні економічної безпеки підприємства і має завжди перебувати в зоні підвищеної уваги з боку керівництва підприємства.

У сучасному світі, де інформаційні технології отримують все більш важливу роль у всіх сферах життєдіяльності людини (особливо у бізнесі), гарантія безпеки інформації стає критичною вимогою для сталого розвитку суспільства взагалі та його економічних складових зокрема. Загрози з боку кіберзлочинців, несанкціонований доступ до даних, виток інформації та інші ризики вимагають від компаній ефективного управління інформаційною безпекою. Таким чином інформаційна безпека – це важливий аспект захисту бізнесу та забезпечення його безперервності.

Засобами захисту інформації називають пристрої, прилади, пристрої, програмне забезпечення, організаційні заходи, які запобігають витоку інформації та забезпечують її збереження в умовах впливу всього спектра

актуальних загроз.

Для захисту даних у сучасних мережах використовується широкий спектр спеціалізованого програмного забезпечення. Можна виділити такі типи програмних засобів захисту.

• Антивірусні програми.

• Хмарні антивіруси (CloudAV).

• Рішення DLP.

• Системи криптографії.

• Міжмережеві екрани (МСЕ).

• Віртуальні приватні мережі VPN.

• Проксі-сервер.

• Рішення SIEM – системи моніторингу та управління інформаційною безпекою.

Великі підприємства агропромислового комплексу, як комерційні, так і державні, мають значний досвід дотримання інформаційної безпеки в умовах обмежених ресурсів. У більшості випадків служби безпеки та охорони займаються цими питаннями окремо.

Однак для малих та середніх підприємств (МСП) такий підхід неможливий через їхні розміри та витрати. Керівництво таких підприємств вважає за краще економити на заходах інформаційної безпеки, що може призвести до значних фінансових і моральних втрат і навіть руйнування бізнесу.

З огляду на вищезазначене, розробка та вдосконалення інструментарію та методичного інструментарію оцінки інформаційної безпеки та впровадження заходів інформаційної безпеки на підприємствах агропромислового комплексу є актуальним питанням.

РОЗДІЛ 2
ОЦІНКА СТАНУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРИКЛАДІ ТОВ «МХП-УРОЖАЙНА КРАЇНА»

2.1. Загальна характеристика діяльності ТОВ «МХП-Урожайна країна».

ТОВ «МХП-Урожайна країна» - підприємство Сумської області, що займається вирощуванням сільськогосподарської продукції.

Компанія обробляє понад 32 000 гектарів землі в Сумській області. Він вирощує зернові та промислові культури, переважно пшеницю, ріпак, кукурудзу, соняшник, горох та сою. У 2021 році на території компанії було зібрано понад 184000 тонн зерна. ТОВ «МХП-Урожайна країна» створено в 2010 році. Компанія входить в агропромислову структуру МХП. І здійснює діяльність на території Сумської області. У 2015 році-увійшло до рейтингу найприбутковіших сільськогосподарських підприємств з вирощування зернових культур.

Компанія належить до господарств з динамічним, високотехнологічним та інноваційним сучасним стилем розвитку з урахуванням особливостей та реалій бізнесу. На сьогоднішній день землі в цьому районі знаходяться у віданні громад Роменського, Недригайлівського, Липоводолинського та Білопільського районів. Відповідно, в структурі ТОВ «МХП-Урожайна країна» є 7 структурних одиниць: Білопільський підрозділ - 4506,1 га; Галківський підрозділ - 2658,7 га; Л.-Долинський підрозділ - 1396,7 га; Смілівський підрозділ - 3602,5 га; Пустовійтівський підрозділ – 4480, 63 га; Хоминцівський підрозділ - 6709,3 га; Глинський зерноочисний комплекс. Виконавчий директор підприємства – Суходольський Олександр Олегович. На підприємстві працює понад 300 осіб.

Підрозділи:

Виробничий підрозділ Суми – 9,9 тис. га;

Виробничий підрозділ Ромни — 22,4 тис. га.

Глинський зерноочисний комплекс — сушіння зерна 40 т/год, очищення 50 т/год.

Потужності підприємства на сьогоднішній день включають:

– рослинницькі підрозділи

– 1 зерноочисний комплекс

– Будівельна бригада

– Парк сільськогосподарської техніки (32 одиниці)

– Потужності для зберігання, сушіння, очищення зерна.

Показники урожайності підприємства за 2022 р. висвітлені в табл. 2.1.

Таблиця 2.1

Урожай за культурами, чистий збір, т

Соняшник	21 302
Соняшник високоолеїновий	7 288
Соя	6 868
Кукурудза	810 000
Пшениця озима	11 034

Джерело: [72]

Земельний банк «МХП-Урожайна країна» становить 32,3 тис. га. Сівозміна в сезоні-2023 була така:

Кукурудза – 11 тис. га (врожайність – 10,5 т/га при плані 9).

Соняшник –7200 га, із них 3300 га – високоолеїновий (врожайність – 2,4 т/га при плані 3,25).

Соя – 6700 га (врожайність – 3 т/га при плані 2,87).

Озима пшениця – 3310 га (врожайність – 6,8 т/га при плані 6,1).

Озимий ріпак – 1379 га (врожайність – 4 т/га при плані 3,2).

Гірчиця – 1115 га (врожайність – 1,23 т/га при плані 1,4).

Гречка – 513 га (врожайність – 2,2 т/га при плані 1,5 т/га).

Підприємство забезпечує усі необхідні умови для працівників:

- пільгове харчування;
- матеріальна допомога при захворюванні працівника чи члена сім'ї працівника (перша лінія спорідненості), якщо лікування потребує значних матеріальних коштів;
- матеріальна допомога при народженні чи усиновленні дитини, смерті працівника чи члена сім'ї працівника (перша лінія спорідненості).

Податкові відрахування до бюджетів усіх рівнів спільно з філією – «МХП – Андріяшівський елеватор» становили 93 484 868,36 грн.

Загальний бюджет КСВ – 5 280 596,69 грн.

Профілем бізнесу «МХП-Урожайна країна» є виробництво зернових та олійних культур. Сільгоспкультури, що здебільшого використовуються на підприємстві є озима пшениця, соя, кукурудза, соняшник та ін.

Види діяльності:

Основний КВЕД: 01.11 Вирощування зернових культур (крім рису), бобових культур і насіння олійних культур.

Інші:

01.61 Допоміжна діяльність у рослинництві

01.63 Післяурожайна діяльність

10.41 Виробництво олії та тваринних жирів

10.61 Виробництво продуктів борошномельно-круп'яної промисловості

46.21 Оптова торгівля зерном, необробленим тютюном, насінням і кормами для тварин

46.71 Оптова торгівля твердим, рідким, газоподібним паливом і подібними продуктами

47.30 Роздрібна торгівля пальним

52.10 Складське господарство

45.11 Торгівля автомобілями та легковими автотранспортними засобами

45.19 Торгівля іншими автотранспортними засобами

46.32 Оптова торгівля м'ясом і м'ясними продуктами

46.33 Оптова торгівля молочними продуктами, яйцями, харчовими оліями та жирами

46.90 Неспеціалізована оптова торгівля

49.41 Вантажний автомобільний транспорт

33.12 Ремонт і технічне обслуговування машин і устаткування промислового призначення

33.17 Ремонт і технічне обслуговування інших транспортних засобів

33.19 Ремонт і технічне обслуговування інших машин і устаткування

ТОВ «МХП Урожайна країна» входить до агропромислового холдингу МХП. Холдинг МХП є значним учасником аграрному ринку. Його виробничі потужності розташовані у 12 областях України. Земельний банк підприємства складається з 360 000 га землі, з них під вирощування сільськогосподарських культур виділена переважна більшість земель- 353000 га. МХП також є одним з найбільших роботодавців в країні, де сьогодні працює більше 32 тисяч людей.

Організаційна схема «МХП МХП-Урожайна країна» представлена в Додатку А.

Розглянемо детальніше основні процеси бізнес-моделі ТОВ «МХП», в якому ТОВ «МХП-Урожайна країна» є однією із складових комплексу ТОВ «МХП»:

1. Вирощування зерна. Компанія має мету забезпечувати увесь процес виробництва комбікормів власними силами.

2. Виробництво соняшникового протеїну. ТОВ «МХП» має унікальний власний виробничий процес вирощування курятини, в якому використовується спеціальна технологія отримання протеїну з насіння соняшнику.

3. Виробництво комбікормів. Власні зернові у виробництві комбікормів, збагачених протеїном, вітамінами і мінералами виробляються на підприємстві з 2020 року.

4. Вирощування бройлерів. Усі підприємства в’язня з виробництвом курятини працюють в замкнутому циклі. Кожен процес автономний та поділений на складові: вирощування курчат бройлерів, інкубатори, сучасні комплекси з переробки та комбікормові заводи.

5. Біогаз. ТОВ «МХП» має на меті вирішення наступних завдань:

- енергетична незалежність;
- виробництво екологічно чистих органічних біологічних добрив;
- суттєве покращення екології в місцях розташування підприємства.

6. М’ясопереробка. Компанія має широкий асортимент продуктів від копченої курки до яловичини преміум-класу та фуа-гра.

7. Дистрибуція. Відправка м’ясної продукції через 14 розподільчих центрів і за допомогою 490 вантажівок-рефрижераторів є останнім етапом вертикальної інтеграції. На цьому етапі забезпечується контроль над якістю продукції від виробничих потужностей до точки продажу.

8. Продаж. Близько 40% продажів проходять через 2940 власних магазинів. Кожен розподільний центр має достатні складські приміщення і власний автопарк. Компанія постачає продукцію усім провідним мережам супермаркетів [91].

Вирощування власних зернових культур – одна з найважливіших структур усієї бізнес-моделі МХП. На полях підприємства вирощуються наступні сільськогосподарські культури: кукурудза, соняшник, пшениця, соя та ріпак. Компанія повністю забезпечує себе власним матеріалом для виробництва власних комбікормів. Це дозволяє контролювати якість та біологічну безпеку при годуванні курей на підприємствах МХП.

Бізнес холдингу МХП складається з одинадцяти рослинницьких підприємств, трьох заводів з виробництва комбікормів та переробки соняшника, заводу з переробки сої та з 14 елеваторів для зберігання продукції. МХП у своїй діяльності активно використовує інноваційні технології в агропромисловому секторі, та розвиває корпоративну культуру в

кращих традиціях міжнародних практик.

Агрохолдинг МХП використовує кілька стратегій, які спрямовані на захист навколишнього середовища. З одного боку це збільшення частки обробітку ґрунту без глибинного втручання та економне поводження з рослинним сміттям. З іншого боку - впровадження та адаптація новітніх технологій вертикальної обробки ґрунту та стрічкової обробки. Розробляється також технологія використання покривних культур для збереження ґрунту.

Крім того, з 2020 року компанія розширила програму використання органічних добрив і у своїй діяльності збільшує відсоток дієвих мікробіологічних препаратів. Це робиться задля покращення якості ґрунтів і дотримання фіто-санітарних умов. Такий підхід до сівозміни забезпечує встановлення корисного симбіозу між мікроорганізмами ґрунту та культурами, що в ньому вирощуються. Щодо мінеральних добрив, то їх використовують у мінімальних кількостях, із застосуванням місцевих особливостей. У той же час на землях, які використовує МХП, проводяться постійні рекультиваційні роботи: для поліпшення ґрунту використовуються природні лікувальні засоби [91].

Попри російсько-українську війну холдинг МХП продовжує розвиватись та інвестує власні кошти у власний бізнес, та створює нові робочі місця в різних куточках України. Під час повномасштабного вторгнення МХП побудував та запустив елеватор у Львівській області. Це підприємство вже розпочало свою роботу та здатне приймати зернові культури, вирощені на підприємствах західних філій холдингу МХП. Потужності елеватора - 1750 тонн пшениці на добу, кукурудзи - 1110 тонн при сушінні від 24 -14 % вологості. Технологічні потужності елеватора передбачають також сушіння та зберігання зерна у полімерних рукавах.

МХП вважає, що соціальна згуртованість та інтеграція демобілізованих залежить не тільки від держави, а й від бізнесу. Компанія заявила, що це спільне завдання та виклик для всіх сімей, бізнесу та уряду.

Відновлення держави також є проблемою для всіх.

Таким чином, у 2022 році сільськогосподарські виробники запустили проект «МХП - поруч», в рамках якого вони надають всебічну підтримку військовим, від мобілізації до реінтеграції в цивільне життя. Сім'ям військових також надається підтримка в соціальній, психологічній та фізичній реабілітації. Мета проекту - реінтеграція демобілізованого персоналу після повернення з військової служби з урахуванням змін фізичного і психічного стану [91].

З початку повномасштабної війни в різних структурних підрозділах ТОВ МХП працювало понад 2300 робітників, які були мобілізовані з початком повномасштабного вторгнення росії. Їм, після мобілізації надається систематична підтримка, від виплати заробітної плати до підтримки військових частин, де вони проходять службу. Пораненим доступний увесь спектр послуг від медичної допомоги до догляду за їхніми сім'ями. Керівництво компанії вважає, що такий проект дуже потрібен зараз. Всебічна підтримка надається кожному ветерану в питаннях адаптації, правових питань, професійної підготовки, реабілітації, психологічної та медичної реабілітації, розвитку соціальних відносин.

Нещодавно МХП отримала International Business Culture Award. Це одна з найпрестижніших відзнак в галузі корпоративної культури. У 2023 році вона відзначалася у 8-ий раз . Премію отримали компанії які досягли найбільших успіхів у створенні виняткової корпоративної культури. Awards and Events спочатку був заснований Тімом Пойнтером, директором з персоналу з 25-річним досвідом керівництва, який керував трансформацією бізнесу (двозначне зростання, злиття, поглинання та IPO) у глобальних організаціях. Його пристрасть до виняткової культури як основи для прискорення ефективності бізнесу призвела до попереднього визнання для нього та його команд і бажання сприяти більшому вивченню, святкуванню та визнанню культури компанії.

На підприємстві МХП діє програма підтримки військових, ветеранів

та їхніх родин “МХП - поруч”. Саме вона перемогла у номінації Best CSR Initiative. Це міжнародна нагорода, яка оцінює внесок організацій у створення та підтримку високоефективної корпоративної культури. Оцінювало журі, у складі якого понад 50 світових бізнес-лідерів.

На сьогоднішній день МХП співпрацює з громадами й громадськими організаціями, що діють на тих територіях, де розташовані землі компанії. Мета такої спів дії - стимулювати розвиток ветеранського бізнесу. Так, створений за кошти агропідприємства благодійний фонд "МХП-Громаді" разом з Українським ветеранським фондом при Міністерстві ветеранів України з квітня 2023 реалізує програму “Варто РОБИти своє”. У межах цього проекту ветерани та їхні родини вже отримали 10 грантів загальним розміром до 15 млн. грн.. які призначені для розвитку власного бізнесу [91].

За підтримки благодійного фонду «МХП-Громаді» на Вінниччині запустили проект з розвитку ветеранського мікробізнесу. Місцеві ветерани та члени їх родин мають можливість пройти професійне, та безоплатне навчання базовим основам ведення малого бізнесу. За результатами навчання вони можуть отримати грант від фонду на суму до 100 000 грн для розвитку власної справи.

Експерти МХП долучаються до подібних проектів як експерти, та надають іншу вагому підтримку - в логістиці, доставці тощо. В компанії вважають, що великий бізнес тільки тоді буде успішним, якщо будуватиме навколо себе розгалужену мережу з взаємопов’язаних малих і середніх бізнесів.

Сівбу озимих культур для збору врожаю у 2024 року вже завершено. Цього року було засіяно 3700 гектарів озимої пшениці. Розпочали сіяти 03.09 і закінчили 31.09. Дощі минулої осені змусили чекати 3 тижні, тому посадили його в посушливу місцевість, щоб він підріс до дощу.

Було посіяно 2812 гектарів насіння озимих овочів, з яких 600 гектарів було випробувано з використанням технології стрічкового культиватора Мзурі, 500 гектарів - з допомогою сівалок безперервної дії Pottinger, 100

гектарів - з допомогою сівалок точного посіву з чергуванням врожаю, розташованих на відстані 70 см один від одного, а решта - на відстані 35 см.

Ферми щороку експериментують із методами посіву, внесення добрив і навіть обробітку ґрунту, щоб знайти найкращий варіант для своїх умов. Ферми почали відмовлятися від плугів на користь відмови від оранки, особливо через нестачу вологи в ґрунті.

У Роменському районі Сумської області, де знаходиться компанія, річна кількість опадів цього року досягла 550 мм вологість в цілому зберігається цілий рік, але неможливо передбачити, коли вона впаде.

Вирощування ведеться в основному під ріпаком, на 30% площі. Вирощування на інших культурах передбачає тільки розпушування, технологію до смуги, деякі мінімальні операції. Ґрунтуючись на даних, що вимірюють продуктивні запаси вологи в метричному шарі ґрунту, ферма порівняла результати оранки і розпушування. Виходить, що різниця становить 30 мм вологості в декаметровому шарі ґрунту, який захищається розпушуванням. А 30 мм - це ще 1 т / га кукурудзи. У 2021 році розпочалися роботи на соєвій ділянці, і було засіяно 2500 гектарів. Сподобалася технологія, тому цього року я посадив 3400 жовтнів сої та ще 600 гектарів ріпаку.

Після збору врожаю стерня відкладається, а навесні надходить в агрегат kuhn excellent для вертикальної обробки, яка розподіляє рослинні залишки по поверхні, а потім жовтень. Ми також спробували шматочки кукурудзи. Рослинні залишки запобігають пересихання ґрунту. Деструктори стерні використовуються для мінералізації рослинних залишків і зниження тягаря хвороб, пов'язаного з насиченням сівозміни соняшником і соєю [91].

На кожному з підприємств МХП є штатний еколог або особа, яка згідно з наказом керівництва відповідає за охорону навколишнього середовища. Ми довіряємо цю роботу тільки фахівцям, які пройшли курси підвищення кваліфікації, успішно склали іспити та отримали сертифікати встановленого зразка.

Щодня фахівці з охорони навколишнього середовища займаються вирішенням таких питань:

- дотримання вимог природоохоронного законодавства
- планомірне зниження формування виробничих і експлуатаційних витрат
- зменшення втрат енергетичних та інших ресурсів, зокрема, обсягів використання води
- зниження впливу холдингових компаній на навколишнє середовище
- запобігання виникненню надзвичайних екологічних ситуацій та аварій, які можуть призвести до значного забруднення довкілля

Вертикально інтегрована бізнес-модель МХП включає комплекси для виробництва біогазу, отриманого з рослинної біомаси, побічних продуктів тваринного походження та стічних вод тощо (Рис. 2.1.).

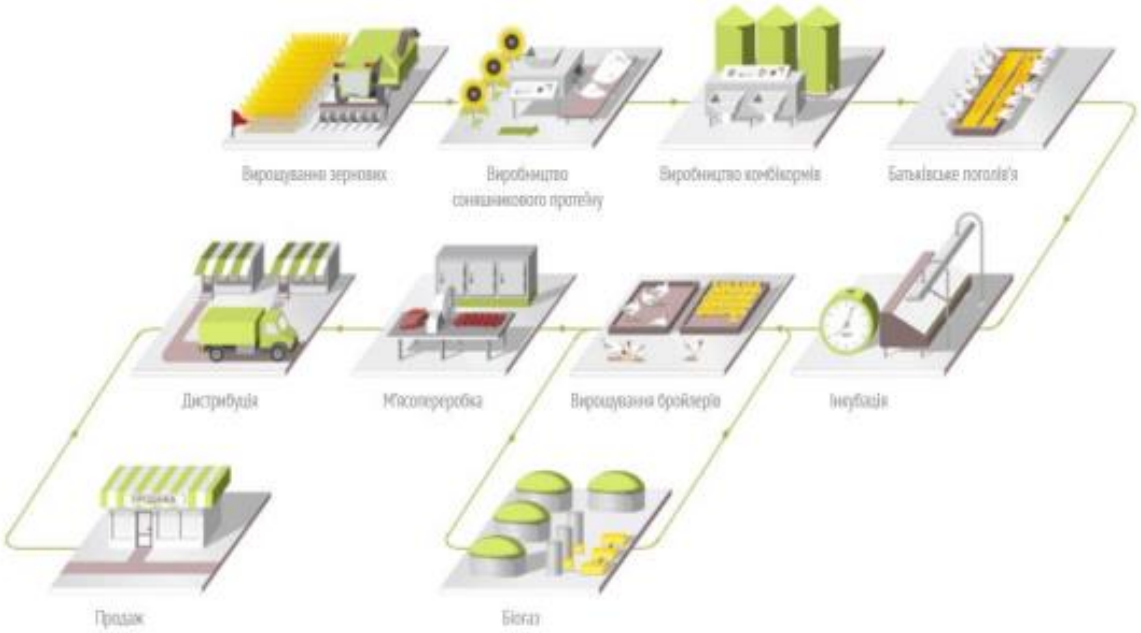


Рис. 2.1. Вертикальна інтеграція ТОВ «МХП»

Джерело: [72]

При цьому на комбікормових заводах переобладнують зерносушарки для роботи на лушпинні соняшнику замість природного газу. Понад рік

працює пілотна установка з виробництва паливних брикетів із зерновідходів. Це дозволяє отримувати паливо з відновлюваних джерел, а також значно зменшити навантаження на місцевий полігон.

Репутація МХП зумовлена його багаторічною діяльністю та поведінкою: те, що ми говоримо і, що ще важливіше, те, що ми робимо; наші бренди та продукти; наші стандарти співпраці; і те, як ми діємо та ставимося до інших. Зміцнюємо довіру. Для МХП, який займає лідируючі позиції на світових ринках, це єдиний спосіб ведення бізнесу. Щоб вести свій бізнес чесно та відповідально, ми маємо бути уважними до ситуацій, які ставлять питання про те, що є правильним і неправильним, і повинні використовувати розсудливість, вирішуючи, який спосіб дій є прийнятним. Наш Кодекс етики має на меті підтримувати цей підхід, будуючись на визнанні того, що все, що ми робимо щодо нашої роботи в МХП, буде і повинно оцінюватися за найвищими стандартами етичної ділової поведінки. Ми встановили таку високу планку з простої причини: наша відданість найвищим стандартам допомагає нам залучати чудових людей, виробляти найкращі продукти та обслуговувати лояльних споживачів. Розглядаємо їх як неймовірну сферу можливостей, основоположну для успіху МНР, і як щось, що ми зобов'язуємося підтримувати щодня. Кодекс етики МХП є загальнодоступним і адресований усім, хто цікавиться діяльністю Компанії та способом її ведення бізнесу. Він містить детальну інформацію про те, як МХП реалізує свої цінності та бачення, а також інструкції для працівників щодо етичних стандартів і способів їх застосування.

2.2. Аналіз основних фінансово-економічних показників діяльності підприємства

Аналізуючи фінансово-економічну діяльність ТОВ «МХП-Урожайна країна» доцільно здійснити розрахунок таких основних фінансово-економічних показників діяльності за 2018-2022 роки. (Табл. 2.2)

Таблиця 2.2

Основні фінансово-економічні показники діяльності ТОВ «МХП-Урожайна країна» за 2018-2022 роки

Показник	2018р.	2019р.	2020р.	2021р.	2022р.	Відхилення (+, –) показника 2021 року порівняно з 2020 роком		Відхилення (+, –) показника 2022 року порівняно з 2021 роком	
						абсолютне	відносне	абсолютне	відносне
А			1	2	3	4	5	6	7
1. Капітал станом на кінець року, тис. грн.:	1495255	1733911	2389445	3230096	2833495	840651	35,18	-396601	-12,28
в т.ч. 1.1. власний капітал:	1339528	1332281	1942162	2169315	2357076	227153	11,70	187761	8,66
1.1.1. власний оборотний капітал	184953	201799	162226	220018	226052	57792	35,62	6034	2,74
1.1.2. нерозподілений прибуток (непокриті збитки)	1154575	1130482	1779936	1949297	2131024	169361	9,52	181727	9,32
Позиковий капітал	155728	401630	447283	1060781	476419	613498	137,16	-584362	-55,09
1.2.1. короткостроковий позиковий капітал	151852	397999	442914	1055380	470838	612466	138,28	-584542	-55,39
1.2.2. довгостроковий позиковий капітал	3876	3631	4369	5 401	5581	1032	23,62	180	3,33
2. Майно станом на кінець року, тис. грн.:	1495255	1733911	2389445	3230096	2833495	840651	35,18	-396601	-12,28
2.1. необоротні активи	339303	357385	300366	373604	385551	73238	24,38	11947	3,20
2.2. оборотні активи:	1155952	1376526	2089079	2856492	2447944	767413	36,73	-408548	-14,30
2.2.1. запаси	560188	348461	783020	737457	523111	-45563	-5,82	-214346	-29,07
2.2.2. дебіторська заборгованість	543783	963530	1199702	1986110	1835206	786408	65,55	-150904	-7,60
2.2.3. грошові кошти та поточні фінансові інвестиції	470	185	69	24	155	-45	-65,22	131	545,83
3. Економічні показники:									
3.1. чистий дохід (виручка) від реалізації продукції (товарів,	699242	108424	810884	1621465	1446987	810581	99,96	-174478	-10,76

Продовж. табл. 2.2

3.2.собівартість реалізованої продукції, тис. грн.	548427	717246	621584	1085541	934915	463957	74,64	-150626	-13,88
3.3. фінансовий результат від звичайної діяльності до оподаткування, тис. грн.	268116	0	610754	136850	158241	-473904	-77,59	21391	15,63
3.4.чистий прибуток (збиток), тис.грн.	268116	0	610754	136850	158241	-473904	-77,59	21391	15,63
3.5.рентабельність (збитковість) обороту, %	38,34	0,00	75,32	8,44	10,94	-66,88	-88,79	2,50	29,57
4. Трудові ресурси:									
4.1.Середньосписк ова чисельність працюючих, осіб	541	433	342	349	356	7	2,05	7	2,01
4.2. Річний фонд оплати праці, тис. грн.	70938	91211	68307	89738	88559	21431	31,37	-1179	-1,31
4.3.Середньомісяч на заробітна плата, грн.	10,93	17,55	16,64	21,43	20,73	4,78	28,74	-0,70	-3,25
4.4. Продуктивність праці, тис. грн./ особу	1292,50	250,40	2371,01	4646,03	4064,57	2275,03	95,95	-581,46	-12,52
5.Фінансові коефіцієнти:									
5.1. автономії	0,896	0,768	0,813	0,672	0,832	-0,141	-17,374	0,160	23,86
5.2.маневрування	0,750	0,734	0,848	0,830	0,839	-0,017	-2,044	0,009	1,027
5.3. фінансового ризику	0,116	0,301	0,230	0,489	0,202	0,259	112,32	-0,287	-58,67
5.4. абсолютної ліквідності	0,003	0,000	0,000	0,000	0,000	0,000	-85,4	0,000	1347,6
5.5. покриття	7,612	3,459	4,717	2,707	5,199	-2,010	-42,62	2,493	92,1

Джерело:[складено автором та розраховано на основі додатків А-Е]

Проаналізувавши дані табл. 2.2 маємо наступні результати. У 2021 р. капітал ТОВ «МХП-Урожайна країна» збільшився на 840651 тис.грн, або на 35,18 %. Це відбулося в основному за рахунок збільшення позикового капіталу на 613498 тис.грн, або більш ніж в 1,37 рази, що складається в основному з короткострокового капіталу. У 2020-2022 роках довгострокові капітальні позики не видавалися.

Обсяг капіталу збільшився на 227153 тис.грн. за рахунок збільшення

нерозподіленого прибутку на 9,52 % у 2021 році, а оборотний капітал залишився незмінним [91]. Зміни розміру капіталу у ТОВ «МХП-Урожайна країна» за 2018-2022 рр. можна продемонструвати на рис. 2.2.

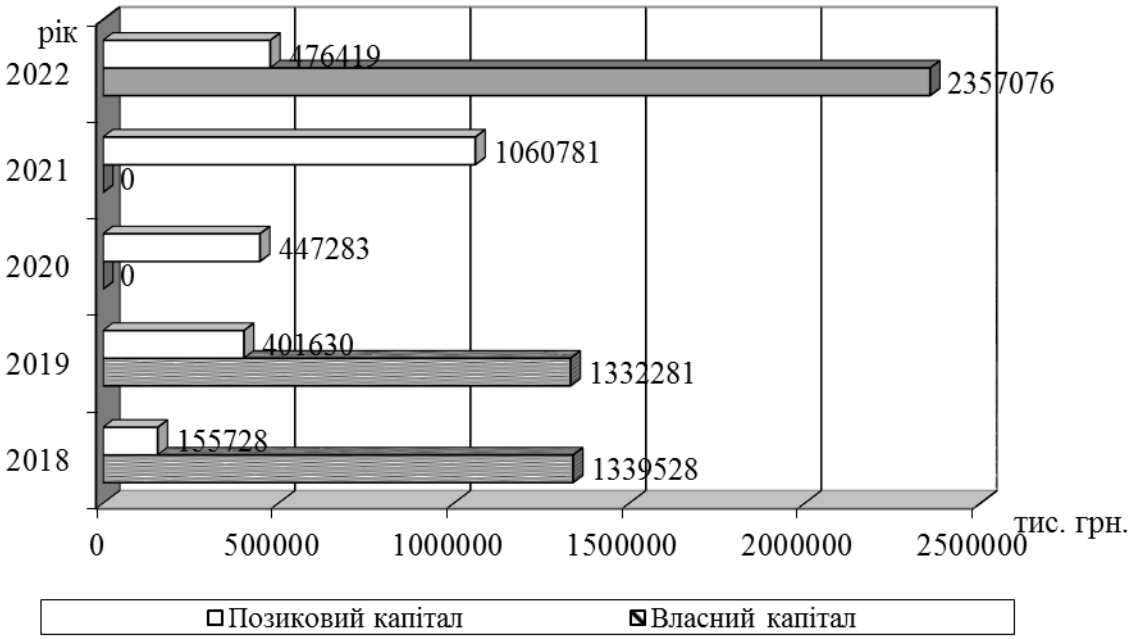


Рис. 2.2. Динаміка розміру капіталу ТОВ "МХП-Урожайна країна" за 2018-2022 рр.

Джерело:[побудовано автором]

У 2022 році капітал скоротився на 12,28%, або на 344570 тис.грн. Позикові кошти збільшилися на 55,09%, або на 584362 тис.грн. Власний капітал зріс на 8,66%, або на 187761 тис.грн, за рахунок зростання нерозподіленого прибутку до 181727 тис. грн., або на 9,32% тис. грн., а власний оборотний капітал зріс на 6034 тис.грн., або 2,74% [91].

Динаміку змін активів ТОВ «МХП-Урожайна країна» у 2018-2022 роках можна продемонструвати на Рис. 2.3.

Велика частина майна компанії - це необоротні активи, які генеруються за рахунок щорічного збільшення основних засобів. У 2021 р. грошові кошти скоротилися на 45 тис.грн, а в 2022 році їх розмір зріс в 5,5 рази і досяг 155 тис. грн.

У 2022 році дебіторська заборгованість знизилася на 7,6% до 1835,206

тис.грн. У 2020 році у компанії був акумульований великий обсяг запасів - 783020 тис.грн, але в 2021 році він знизився на 5,82% і знизився ще на 29,07% до 523 111 тис. грн в 2022 році .

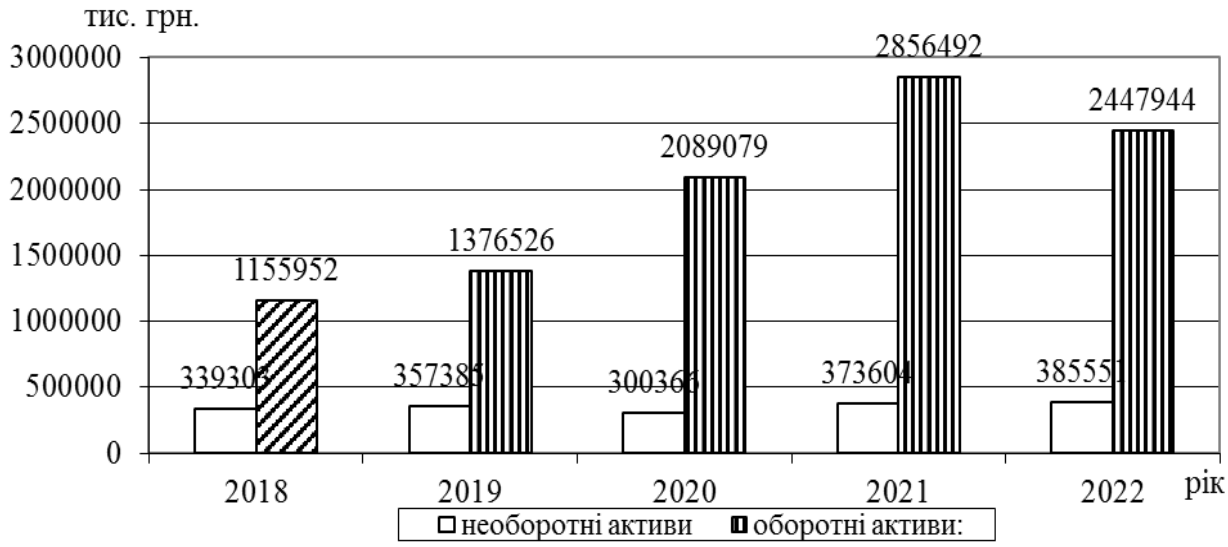


Рис. 2.3. Динаміка зміни розміру активів ТОВ "МХП-Урожайна країна" за 2018-2022 роки

Джерело:[побудовано автором]

Беручи до уваги економічні показники, наведені в таблиці 1.1, можна зробити наступні висновки.

Чистий дохід у 2021 році зріс майже в 2 рази порівняно з 2020 роком, але дещо знизився у 2022 році, знизившись на 10,76% порівняно з попереднім роком. Так, у 2021 році порівняно з 2020 роком собівартість продукції значно зросла на 74,64%, або на 463957 тис.грн. У 2022 році собівартість знизилася такими ж темпами, як і чистий дохід - вона знизилася на 13,88%, або на 150626 тис.грн.

Графічно динаміку змін основних показників фінансових результатів ТОВ «МХП-Урожайна країна» у 2018-2022 роках можна проілюструвати на рисунку 2.3.

Як видно з рис. 2.4, компанія отримує чистий прибуток у 2020-2022 роках. У 2021 році компанія втратила 77,59% чистого прибутку, або 473904

тис.грн, на що вплинуло значне зростання виробничих витрат.

Чистий прибуток у 2021 році склав 15,63%, що на 158241 тисячі гривень більше, ніж у 2022 році, коли підприємство отримало інші доходи.

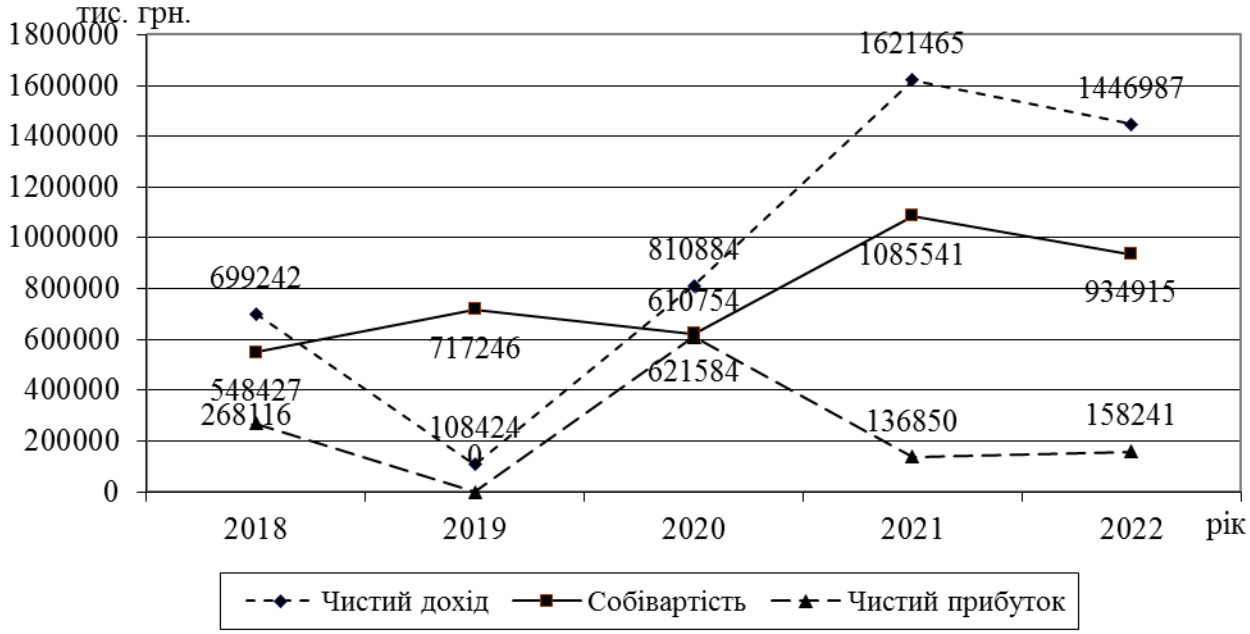


Рис. 2.4. Динаміка змін розмірів основних показників фінансових результатів ТОВ «МХП-Урожайна країна» за 2018-2022 рр.

Джерело:[побудовано автором]

Як бачимо з графіку, основні результативні показники , такі як чистий дохід та чистий прибуток стрімко зростали до 2021 року, але в 2022 році вони знизились, і до цього є цілком логічне пояснення, це, перш за все пов’язано з широкомасштабним вторгненням ворога в нашу країну та активними військовими діями, в тому числі і у ареалі здійснення господарської діяльності підприємства.

Середньоспискова чисельність персоналу підприємства в період з 2018 по 2022 рік залишалася стабільною, їх кількість поступово збільшувалася на 7 осіб у 2021 році та на 7 осіб у 2022 році [72].

Середньомісячна заробітна плата постійно зростає і в 2022 році збільшилася на 28,74%, що мало вплив на активну роботу персоналу і складе 6140 грн. на одного працівника.

В результаті продуктивність праці персоналу зросла з 693 тис.грн./особу у 2020 році до 1141 тис. грн./особу у 2022 році.

Розрахунок фінансових коефіцієнтів може бути графічно відображений на рисунку 2.5.

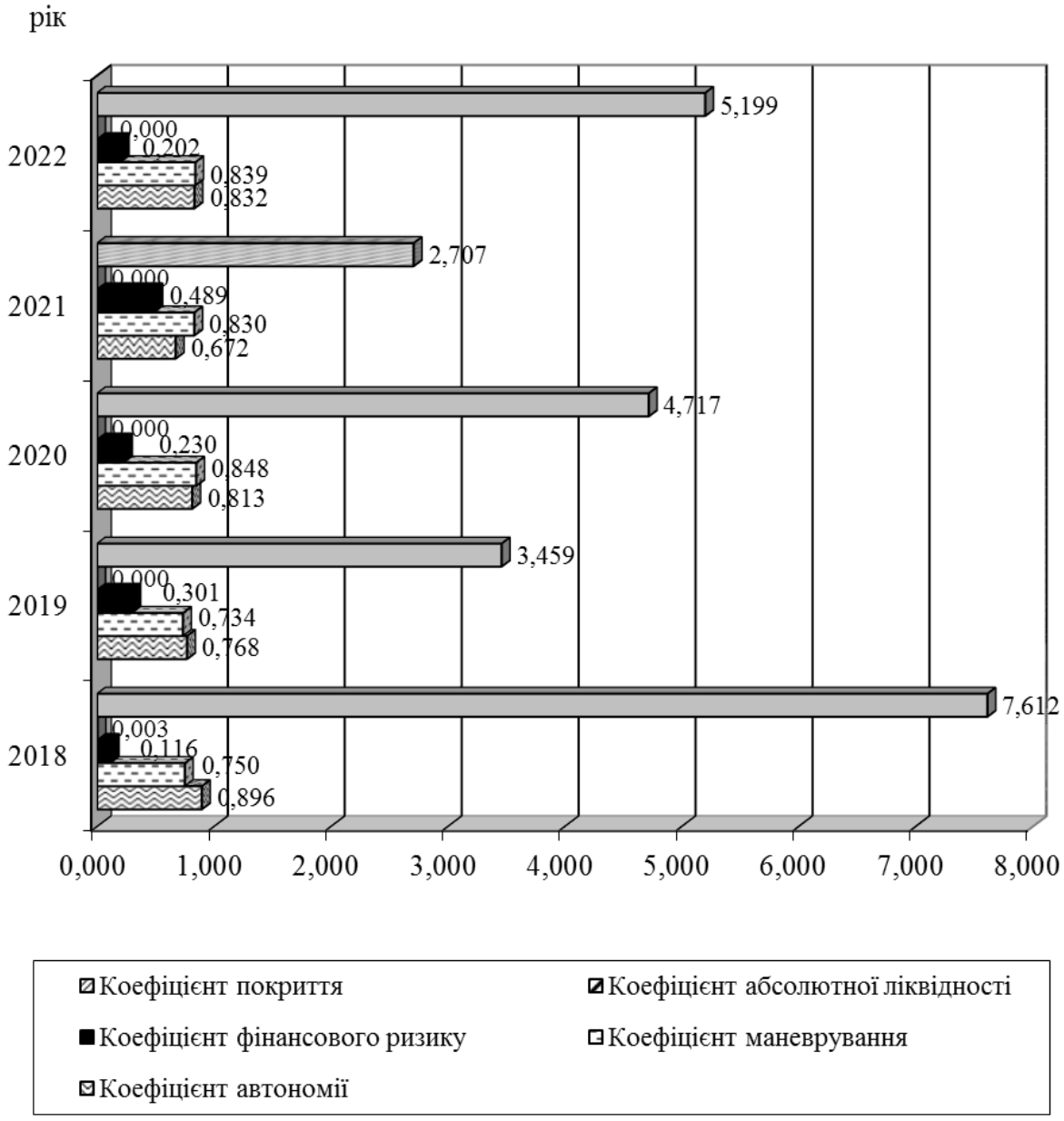


Рис. 2.5. Зміна фінансових коефіцієнтів ТОВ "МХП-Урожайна країна" за 2018-2022 роки.

Джерело:[побудовано автором на основі розрахунків]

Як видно з рис. 2.5, з 2018 по 2022 році всі показники покращилися, але показник маневреності відсутній. У 2022 році всі показники значно

підвищилися - автономність на 23,86%, покриття - на 92,1%, а коефіцієнт фінансового ризику знизився - на 58,67%.

Розглянемо коефіцієнти ліквідності в таблиці нижче (табл. 2.3).

Таблиця 2.3

Аналіз ліквідності ТОВ "МХП-Урожайна країна" на 2018-2022 роки

Показник	Джерело інформації	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.	Відхилення +/- 2022 р. від 2018р.	Відхилення +/- 2022 р. від 2021р.
1	2			3	4	5	6	7
1. Коефіцієнт поточної ліквідності (Кпл)	$\frac{ф.1,\ р.1195}{ф.1,\ р.1695}$	7,61	3,46	4,72	2,71	5,20	-2,4	2,49
Коефіцієнт швидкої квідності (Кшл)	$\frac{ф.1,\ р.1195 - р.1100 - р.1110}{ф.1,\ р.1695}$	3,74	2,55	2,90	1,99	4,01	0,3	2,02
3. Коефіцієнт абсолютної ліквідності (Кал)	$\frac{ф.1,\ р.1160 + р.1165}{ф.1,\ р.1695}$	0,00	0,00	0,00	0,00	0,00	0,0	0,00
4. Власні оборотні кошти (ВОК)	*ф.1, р. 1495 – ф.1, р.1095*	1000225	974896	1641796	1795711	1971525	971300	175814
5. Коефіцієнт забезпеченості власними оборотними коштами (Квок)	$\frac{ф.1,\ р.1495 - р.1095}{ф.1,\ р.1195}$	0,87	0,71	0,79	0,63	0,81	-0,1	0,18
6. Коефіцієнт забезпеченості запасів і витрат власними оборотними коштами (Кзвок)	$\frac{ф.1,\ р.1495 - р.1095}{ф.1,\ р.1100 + 1110}$	1,70	2,68	2,04	2,37	3,51	1,8	1,14
7. Коефіцієнт маневреності власних оборотних коштів ($Кман_{вок}$)	$\frac{ф.1,\ р.1165}{ф.1,\ р.1495 - ф.1,\ р.1095}$	0,00	0,00	0,00	0,00	0,00	0,0	0,00
8. Коефіцієнт покриття запасів (Кпокр.зап)	$\frac{ф.1,\ р.1495 - р.1095 + + р.1600 + р.1615}{ф.1,\ р.1100 + р.1110}$	1,77	2,92	2,13	2,51	3,60	1,8	1,09

Джерело:[складено автором на основі розрахунків]

Наведені в таблиці розрахунки показують, що найбільше значення показник ліквідності мав у 2018 році, потім вона суттєво знизилась через ряд негативних факторів, проте в наступному періоді вона поступово зростала і навіть збільшилась вдвічі протягом 2021-2022 рр. Динаміка основних

показників ліквідності ТОВ "МХП-Урожайна країна" в 2018-2022 роках показана на рисунку 2.6.

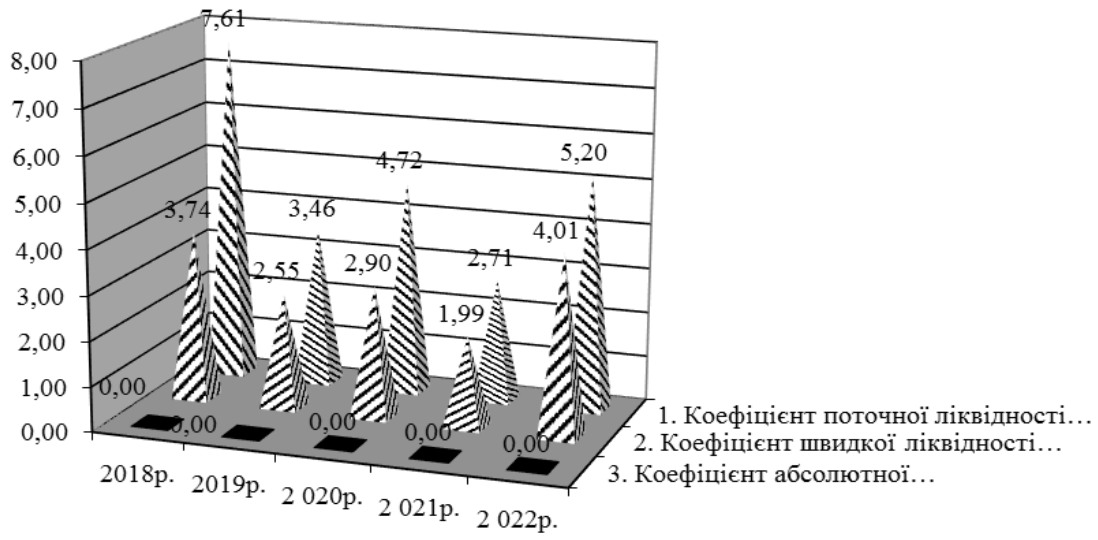


Рис. 2.6. Динаміка показників ліквідності
ТОВ "МХП-Урожайна країна" у 2018-2022 роках

Джерело:[побудовано автором на основі розрахунків]

Як видно з рис. 2.6, у 2022 році коефіцієнт швидкої ліквідності покращився на 2,02 процентного пункту, а поточна ліквідність - на 2,49 процентного пункту. Через невеликий розмір грошових коштів та їх еквівалентів коефіцієнт абсолютної ліквідності дуже низький, його значення не змінилося в 2022 році і становить 0,002 .

Наступник кроком в процесі аналізу фінансово-економічного стану досліджуваного в даній кваліфікаційній роботі підприємства є оцінка показників фінансової стійкості.

Обчислення показників, які характеризують фінансову стійкість дозволить визначити надлишок, або навпаки - нестачу основних джерел фінансування, обсяги запасів на підприємстві, можливість забезпечення цих запасів із власних обігових коштів, а також необхідність залучення

кредитних коштів, зокрема, короткострокових кредитів банків, якщо у тому виявиться потреба. Отже, необхідні для обчислення показників фінансової стійкості данні згрупуємо у вигляді таблиці (табл. 2.4).

Таблиця 2.4

Аналіз показників фінансової стійкості

ТОВ "МХП-Урожайна країна" у 2018 - 2022 роках

Показник	Джерело інформац (форма № 1)	2018 рік, тис.грн	2019 рік, тис.грн	2020 рік, тис.грн	2021 рік, тис.грн	2022 рік, тис.грн	Відхилення (+, –) показника 2022 р. порівняно з 2018 р.		Відхилення (+, –) показника 2022 р. порівняно з 2021 р.	
							Абсолют тис.грн.	Відн., %	Абсолют. тис.грн.	Відн., %-ти
1. Постійні пасиви (ПП)	р. 1495	1339528	1332281	1942162	2169315	2357076	1017548	75,96	187761	8,66
2. Активи, що важно реалізуються ($А_{ВР}$)	р. 1095	339303	357385	300 366	373604	385551	46248	13,63	11947	3,20
3. Власні обігові кошти (ВОК)	ПП - $А_{ВР}$	1000225	974896	1641796	1795711	1971525	971300	97,11	175814	9,79
4. Довгострокові зобов'язання (ДЗ)	р.1595	3876	3631	4 369	5 401	5581	1705	43,99	180	3,33
5. Наявність постійних та довгострокових	ВОК + ДЗ	1004101	978527	1646165	1801112	1977106	973005	96,90	175994	9,77
6. Короткострокові кредити банків (КК)	р. 1600	0	0	0	0	0	0	0	0	0
7. Загальна сума основних джерел фінансування запасів	ВОК + ДЗ + КК	1004101	978527	1646165	1801112	1977106	973005	96,90	175994	9,77
8 Запаси (З)	р. (1100 + 1110)	587269	363133	803143	756296	561591	-25678	-4,37	-194705	-25,74
9. Надлишок (нестача) власних обігових коштів	ВОК - З	412956	611763	838653	1039415	1409934	996978	241,4	370519	35,65
10. Надлишок (нестача) власних обігових коштів та довгострокових зобов'язань	ВОК + ДЗ-З	416832	615394	843022	1044816	1415515	998683	239,6	370699	35,48
11. Надлишок (нестача) основних джерел фінансування запасів	ВОК + ДЗ + КК - З	416832	615394	843022	1044816	1415515	998683	239,6	370699	35,48

Джерело:[складено автором на основі додатків А-Е]

В результаті оцінок показників фінансової стійкості можна зробити наступні висновки: з 2018 по 2020 рр. компанія перебувала у стабільному фінансовому становищі. У 2021 та 2022 роках ситуація покращилася, і компанія покращила показники фінансової стабільності. Це пов'язано з тим, що запаси підприємства менше за постійні пасиви. За 2022 рік вони зменшилися на 25,74 % або на 194705 тис. грн. і дорівнюють 561591 тис. грн.

Таблиця 2.5

Аналіз показників платоспроможності підприємства ТОВ "МХП-Урожайна країна" за 2018-2022 рр.

Назва показника	Нормативне значення	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.	Відхилення (+, –) показника 2022 р. порівняно з 2018 р.		Відхилення (+, –) показника 2022 р. порівняно з 2021 р.	
							Абсол.	Відн.	Абсол.	Відн.
Коефіцієнт автономії	більше 0,5	0,896	0,768	0,813	0,672	0,832	-0,064	-7,14	0,160	23,86
Коефіцієнт фінансової залежності	менше 0,2	1,116	1,301	1,230	1,489	1,202	0,086	7,69	-0,287	-19,27
Коефіцієнт фінансового ризику	менше 0,5	0,116	0,301	0,230	0,489	0,202	0,086	73,86	-0,287	-58,67
Коефіцієнт маневреності власного капіталу	більше 0	0,747	0,732	0,845	0,828	0,836	0,090	12,02	0,009	1,05
Коефіцієнт структури покриття довгостроко-вих вкладень	-	0,011	0,010	0,015	0,014	0,014	0,003	26,72	0,000	0,13
Коефіцієнт довгострокового залучення коштів	0,4	0,003	0,003	0,002	0,002	0,002	-0,001	-18,13	0,000	-4,89
Коефіцієнт фінансової незалежності капіталізованих джерел	0,6	0,997	0,997	0,998	0,998	0,998	0,001	0,052	0,000	0,012

Джерело:[складено автором на основі розрахунків]

Однією з найважливіших характеристик фінансового стану підприємства є його незалежність від зовнішніх джерел фінансування. Для цієї мети коефіцієнт фінансової незалежності (автономії) розраховується як відношення загальної суми власного капіталу до загальної суми балансу. Згідно з таблицею, компанія була фінансово незалежною у 2018-2021 роках. Тобто могло здійснювати всі платежі за свій рахунок. У 2022 році ситуація була такою ж.

Відношення власних коштів до залучених коштів визначає, чи може підприємство залучити залучений капітал в господарський оборот. У 2020-2022 роках видно, що власних коштів достатньо для покриття ресурсів інших.

На рисунку 2.7 показана динаміка зміни коефіцієнтів фінансової стійкості (платоспроможності) підприємства ТОВ "МХП-Урожайна країна" з 2018 по 2022 рік.

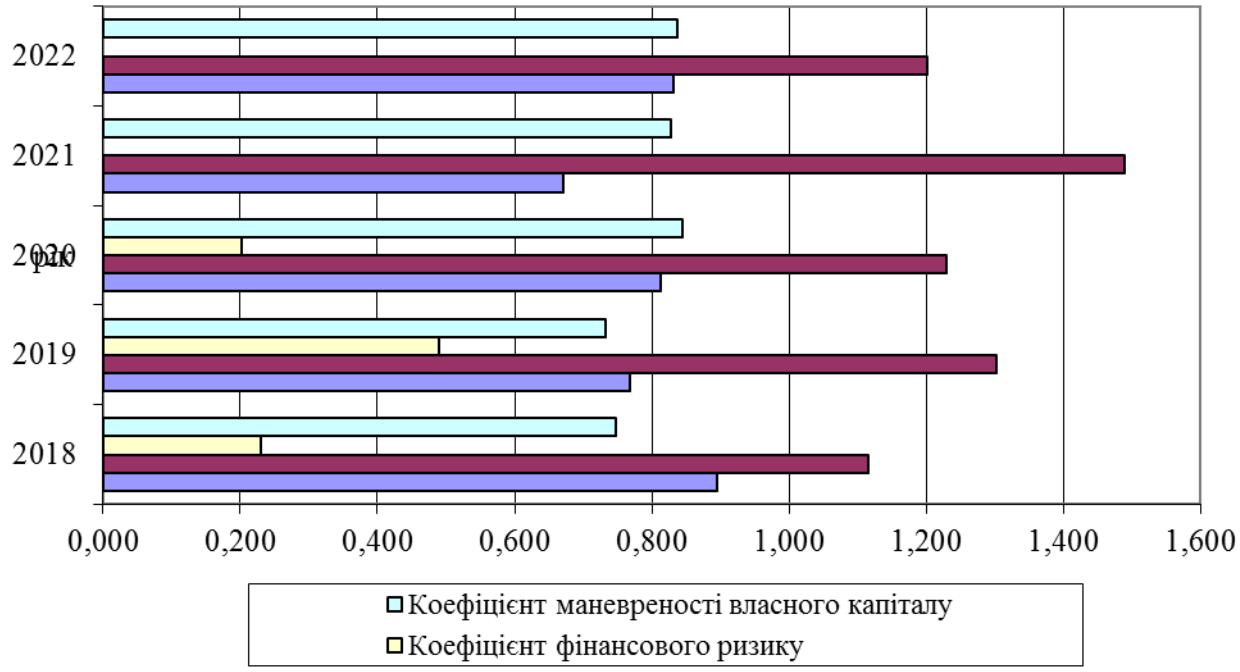


Рис. 2.7. Динаміка змін коефіцієнтів фінансової стійкості (платоспроможності) ТОВ "МХП-Урожайна країна" у 2018-2022 рр.

Джерело:[побудовано автором на основі розрахунків]

Коефіцієнт автономії за період 2018-2021 рр. знизився на 0,224, а в 2022 році збільшився на 0,160 порівняно з 2021 роком.

Коефіцієнт маневреності в 2022 році порівняно з 2021 роком був поліпшений на 0,09, і підприємство є маневреним, а коефіцієнт фінансового ризику зріс з 2018 по 2021 рік на 58,67% [91].

Аналіз коефіцієнтів ділової активності дозволяє проаналізувати ефективність основних видів діяльності підприємства, що характеризуються

швидкістю обороту фінансових ресурсів ТОВ "МХП-Урожайна країна". Аналіз проводиться з використанням коефіцієнта оборотності.

У наступній аналітичній таблиці (табл. 2.6) спробуємо оцінити рівень ділової активність досліджуваного підприємства, ТОВ "МХП-Урожайна країна" за період з 2018 по 2022 рік.

Таблиця 2.6

Аналіз ділової активності ТОВ "МХП-Урожайна країна" у 2018-2022 рр.

Показники	Формула для розрахунку	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.	Відхилення +/- 2022 р. від 2018р.	Відхилення +/-2022 р. від 2021р.
1	2	3	4	5	6	7	8	9
1. Коефіцієнт оборотності активів	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1300_П+1300_К)}$	0,468	0,063	0,339	0,577	0,477	0,010	-0,100
2. Коефіцієнт оборотності основних фондів	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1005_П+1010_П+1005_К+1010_К)}$	2,803	0,431	3,986	6,748	5,029	2,23	-1,719
3. Коефіцієнт оборотності оборотних активів	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1195_П+1195_К)}$	0,605	0,079	0,388	0,656	0,546	-0,06	-0,110
4. Коефіцієнт оборотності запасів	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1100_П+1110_П+1100_К+1110_К)}$	1,191	0,299	1,010	2,080	2,196	1,01	0,116
5. Коефіцієнт оборотності готової продукції	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1103_П+1103_К)}$	1,572	0,484	1,151	2,672	4,240	2,67	1,568
6. Коефіцієнт оборотності дебіторської заборгованості	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1125_П+...+1155_П+1125_К+...+1155_К)}$	1,286	0,113	0,676	1,018	0,757	-0,53	-0,261
7. Коефіцієнт оборотності власного капіталу	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1495_П+1495_К)}$	0,522	0,081	0,418	0,789	0,639	0,12	-0,149
8. Коефіцієнт оборотності кредиторської заборгованості	$\frac{ф.2\ р.2000*2}{ф.1\ р.(1610_П+...+1650_П+1610_К+...+1650_К)}$	5,179	0,307	1,867	2,221	1,954	-3,23	-0,268

Джерело:[складено автором на основі розрахунків]

Як видно з таблиці 2.6, рівень, що характеризує ділову активність з 2018 р. по 2021 р. поліпшується, і всі коефіцієнти збільшуються. У 2022 році комерційна діяльність продовжує поліпшуватися - майже всі коефіцієнти збільшені.

Оборот основних фондів за період з 2018-2022 рр. збільшився на 2,23 процентного пункту, а оборот активів знизився на 0,06 %. Найбільше збільшення відбулося в обороті готової продукції - на 2,6 %.

Водночас зниження показника оборотності готової продукції протягом 2021-2022 рр. свідчить про зростання періоду обігу коштів від початку вкладання їх у виробництво до отримання виручки від реалізації готової продукції, це загальна тенденція на всіх аграрних підприємствах країни, і пов’язана вона, перш за все, з військовою агресією проти нашої країни і значно ускладнений процес реалізації продукції аграрних підприємств.

У таблиці 2.7 здійснимо розрахунок періоду обороту фінансових ресурсів ТОВ "МХП-Урожайна країна" з 2018 по 2022 рік.

Таблиця 2.7

Період оборотності фінансових ресурсів ТОВ "МХП-Урожайна країна" з 2018 по 2022 рік.

Показник	Формула для розрахунку	Напрямок позитивних змін	2018 р., дні	2019 р., дні	2020 р., дні	2021 р., дні	2022 р., дні
1	2	3	4	5	6	7	8
1. Період оборотності активів	$\frac{360}{К_{А}}$	>0, зменшення	769,82	5757,10	1060,82	623,83	754,29
2. Період оборотності основних фондів	$\frac{360}{К_{ОФ}}$	>0, зменшення	128,41	835,39	90,31	53,35	71,58
3. Період оборотності оборотних активів	$\frac{360}{К_{ОА}}$	>0, зменшення	595,13	4570,48	927,47	549,01	659,85
4. Період оборотності запасів	$\frac{360}{К_{З}}$	>0, зменшення	302,35	1205,71	356,56	173,11	163,94
5. Період оборотності готової продукції	$\frac{360}{К_{ГП}}$	>0, зменшення	229,00	744,25	312,76	134,74	84,91
6. Період оборотності дебіторської заборгованості	$\frac{360}{К_{ДЗ}}$	>0, зменшення	279,96	3199,21	532,62	353,66	475,36
7. Період оборотності власного капіталу	$\frac{360}{К_{ВК}}$	>0, зменшення	689,65	4423,57	862,24	456,42	563,07
8. Період обороту кредиторської заборгованості	$\frac{360}{К_{КЗ}}$	>0, збільшення	69,52	1172,54	192,87	162,06	184,25

Джерело:[складено автором на основі розрахунків]

У таблиці 2.7 показано, що коефіцієнт оборотності активів є низьким з 2020 по 2021 роки, оскільки він перевищував 1 рік. За період з 2020 по 2022 рік цей показник суттєво покращився, а точніше - знизився на 306,53 днів. За

2 роки період обороту основних засобів був збільшений до 18,73 дня, зокрема, період обороту готової продукції - до 227,85 дня. Збільшення оборотності теж пов’язана з війною, оскільки продавати зерно стало складніше, через руйнування транспортних ланцюгів в результаті військової агресії у Чорному морі, а також ризик втрати урожаю через обстріли.

Тепер варто перейти до розрахунку показників рентабельності, наведених в таблиці 2.8.

Таблиця 2.8

Показник рентабельності ТОВ "МХП-Урожайна країна" у 2018-2022 роках

Показник	Формула для розрахунку	2018р.	2019р.	2020р.	2021р.	2022р.	Відхилення +/- 2021 р. від 2020р.	Відхилення +/-2022 р. від 2021р.
1	2	3	4	5	6	7	8	9
1. Коефіцієнт рентабельності майна	$\frac{ф.2\ р.2350(2355)*2}{ф.1\ р.(1300_{П}+1300_{К})}$	17,93	0,00	25,56	4,87	5,22	-12,71	0,35
2. Коефіцієнт рентабельності капіталу	$\frac{ф.2\ р.2350(2355)*2}{ф.1\ р.(1900_{П}+1900_{К})}$	17,93	0,00	25,56	4,87	5,22	-12,71	0,35
3.Коефіцієнт рентабельності власного капіталу	$\frac{ф.2\ р.2350(2355)*2}{ф.1\ р.(1495_{П}+1495_{К})}$	39,99	0,00	37,30	6,66	6,99	-32,99	0,33
4.Коефіцієнт рентабельності продаж	$\frac{ф.2\ р.2090(2095)}{ф.2\ р.2000}$	21,57	338,49	23,34	33,05	35,39	13,82	2,34
5. Коефіцієнт валової рентабельності основної діяльності	$\frac{ф.2\ р.2090(2095)*2}{ф.2\ р.2050}$	27,50	51,17	30,45	49,37	54,77	27,27	5,40
6.Коефіцієнт рентабельності операційної діяльності	$\frac{ф.2\ р.2190(2195)}{ф.2\ р.(2050+2180)}$	0,00	25,70	72,71	7,45	1,98	1,98	-5,47
7. Коефіцієнт чистої рентабельності реалізованої продукції	$\frac{ф.2\ р.2350(2355)}{ф.2\ р.2000}$	38,34	0,00	75,32	8,44	10,94	-27,41	2,50
8.Коефіцієнт рентабельності необоротних активів	$\frac{ф.2\ р.2350(2355)*2}{ф.1\ р.(1095_{П}+1095_{К})}$	79,02	0,00	203,34	40,61	41,69	-37,33	1,08
9.Коефіцієнт рентабельності оборотних активів	$\frac{ф.2\ р.2350(2355)*2}{ф.1\ р.(1195_{П}+1195_{К})}$	23,19	0,00	29,24	5,53	5,97	-17,23	0,43

Джерело:[складено автором на основі розрахунків]

В результаті отримання компанією чистого прибутку в період 2018-2022 років показники рентабельності мають позитивне значення і з кожним роком поліпшуються.

На рис. 2.8. показані значення ключових показників рентабельності. У 2022 році чистий прибуток склав понад 21391 тис.грн, тому коефіцієнт рентабельності поліпшується і залишається високим.

Таким чином, виручка від продажів зросла з 21,57 % у 2018 році до 35,39% у 2022 році.

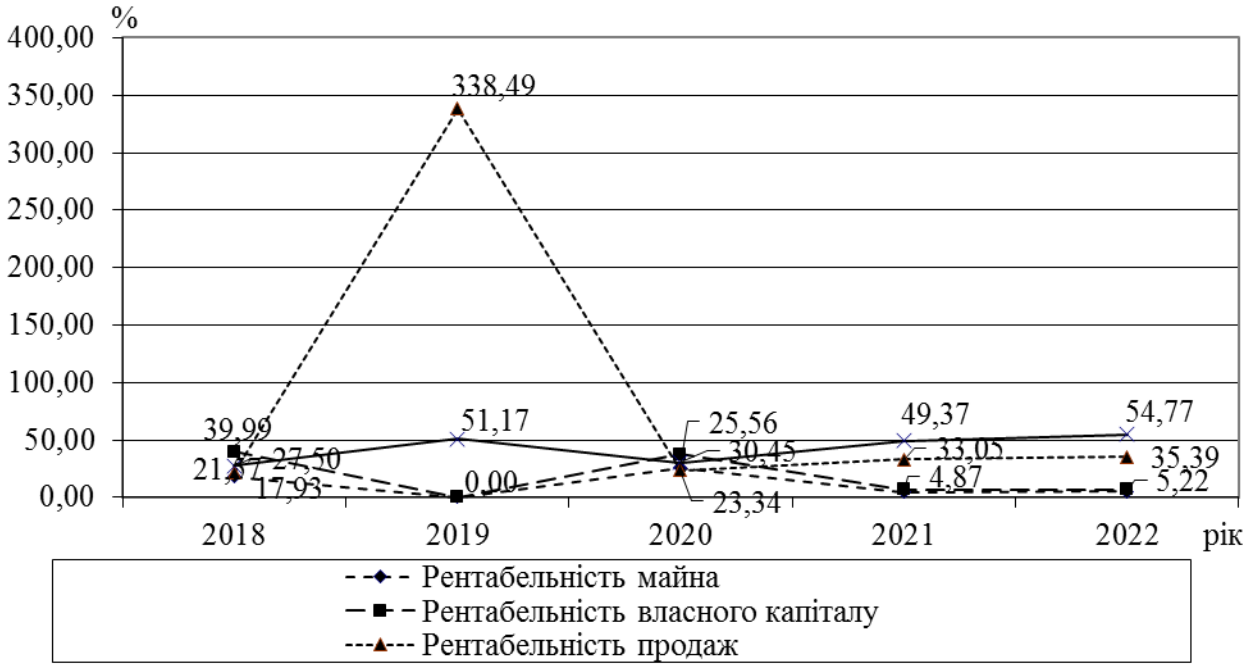


Рис. 2.8. Динаміка основних показників рентабельності ТОВ "МХП-Урожайна країна" за 2018-2022 рр.

Джерело:[побудовано автором на основі розрахунків]

Найбільший показник рентабельності - валова рентабельність основної діяльності становить 54,77%, що на 5,4 процентних пункту більше, ніж у 2021 році.

Таким чином, проведені розрахунки показали, що у 2022 році мають місце позитивні зміни в фінансово-економічній діяльності підприємства. Спостерігається зростання чистого доходу, заробітної плати та чистого прибутку. Поліпшення всіх фінансових показників є позитивним.

2.3 Стан інформаційної безпеки на підприємстві ТОВ "МХП-Урожайна країна"

Якщо великі банки та власники об'єктів критичної інформаційної інфраструктури добре знають, як будувати свою модель ІБ, то 40% українських компаній не мають розуміння стратегії в цьому питанні, вважає найбільша світова аудиторська компанія Price waterhouse Coopers (PwC) [81].

В результаті оцінок компанії виявлено наступні проблеми:

– майже 50% українських компаній не приділяють уваги навчання співробітників основ інформаційної безпеки;

– 56% компаній відмовляються від впровадження системи реагування на інциденти через її економічну, на їхню думку, неефективність;

– лише 19% компаній упевнені в тому, що їхні програмно-апаратні засоби дозволять ідентифікувати винуватця інциденту;

– 25% компаній упевнені в тому, що основний ризик несуть мобільні пристрої співробітників, але не готові впроваджувати програмні рішення щодо знешкодження загрози [81].

Поки керівники компаній лише приходять до думки про необхідність тестування вразливості, даркнет поповнюється пропозиціями щодо продажу даних, які забезпечують доступ до вже зламаних систем захисту.

Експерти припускають, що ситуація з погрозами у 2023-24 роках розвиватиметься за такими напрямками:

- розуміння неможливості побудови ідеальної системи захисту призведе до зростання ринку SIEM-систем, що дозволяють найшвидше виявляти інциденти та реагувати на них;
- посилиться полювання за навченими кадрами, компанії вкладатимуть більше коштів у створення спільних із вузами програм навчання фахівців з кібербезпеки;
- посилиться роль єдиних державних систем керування інцидентами;

- завдяки новим криміналістичним технологіям почнеться виявлення хакерських угруповань, які непомітно контролюють мережі компаній вже кілька років;
- підвищиться роль ОС, які містять відомі вразливості;
- у зв'язку із зростанням захищеності великих компаній підвищиться кількість атак, спрямованих на їх постачальників та підрядників.

Враховуючи ці аспекти та вже опрацьовані приклади впровадження системи інформаційної безпеки підприємства, потрібно вибудовувати стратегію підприємства на найближчі роки.

Для забезпечення успішності процесів управління, необхідно враховувати дію наступних факторів:

1) Невірна інформація, а також її перевищення можуть несприятливо позначитися на системі управління в цілому, викликаючи її розростання, ускладнення, підвищення обсягів трудовитрат адміністративно-управлінського персоналу.

2) Своєчасність надходження до споживачів. Затримка надходження інформації може знизити результативність прийнятих керівниками рішень, уповільнити процес прийняття управлінських рішень.

3) Короткість і змістовність. Дані властивості допомагають прискорити обробку інформації та її доставку.

4) Доступність сприйняття.

У сільському господарстві комп'ютер разом з програмним забезпеченням може виконати великий діапазон функцій і полегшити працю працівників виробництва. помилок і виконання

Питанням побудови та аналізу системи інформаційної безпеки присвячені роботи провідних світових та вітчизняних науковців. У роботах одних авторів наведено велику кількість показників, що характеризують стан інформаційної безпеки, у роботах інших – зазначені заходи щодо підвищення рівня захищеності інформації підприємства, у роботах третіх – пропонуються комплексні методики, які, на жаль, по-перше, дуже важко впроваджувати

через велику кількість складно оцінюваних показників, а з іншого сторони, – нелегко узгодити з чинним законодавством та міжнародними та національними стандартами, що регламентують діяльність, пов'язану з інформаційною безпекою [7].

Таким чином виникла необхідність розробки комплексного показника стану інформаційної безпеки підприємства, з урахуванням методик його розрахунків та визначення критичних значень окремих показників, що демонструють наявний рівень інформаційної безпеки.

В роботі були узагальнені дослідження українських та закордонних вчених, що досліджували різні питання інформаційної безпеки. Висвітлено пропозиції для керівників підприємств агропромислового комплексу про перелік заходів щодо забезпечення відповідного рівня інформаційної безпеки.

Інформаційна безпека будь-якого підприємства демонструється завдяки захищеності його інформаційного середовища та ефективності інформаційного забезпечення всього процесу управління підприємством.

Заходи, що повинні забезпечити інформаційну безпеку можна вважати взаємодією трьох підсистем:

- інформаційне забезпечення усього процесу керування підприємством;
- захист інформаційної мережі та середовища на агропідприємстві;
- діагностування рівня інформаційної безпеки в структурних підрозділах агропідприємства [74].

Головне завдання підсистеми інформаційного забезпечення процесу управління агропідприємством виокремлюється як система до якої входять: збір потрібної інформації; її обробка та систематизація, оцінка та аналіз; прогнозування різних аспектів виробничої та соціальної діяльності підприємства, забезпечення необхідною та достовірною інформацією осіб, які приймають рішення.

Безперервне виконання всіх цих умов призведе до ефективного

функціонування усієї підсистеми.

Захист інформаційного середовища агропідприємства складається як із захисту від шкідливих дій як конкурентів, так і від власних співробітників. Також враховується захист від ненавмисних внутрішніх негативних подій.

Методи та методики дослідження.

Для забезпечення захисту інформаційного середовища підприємства необхідно систематичне виконання наступних етапів (рис. 2.9.):

– аналіз загроз інформаційній безпеці;

– планування та розробка заходів щодо забезпечення інформаційної безпеки;

- оперативна реалізація запланованих дій.

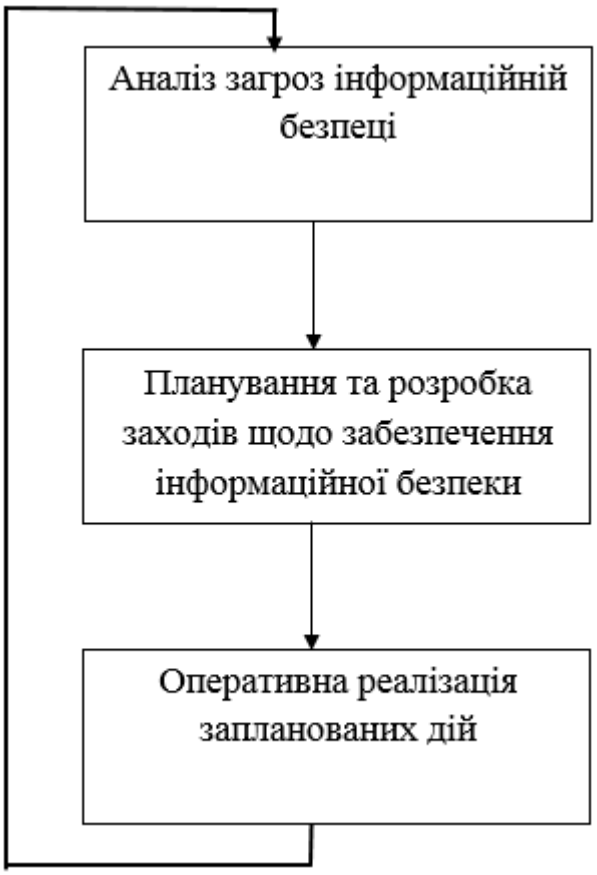


Рис. 2.9. Схема функціонування інформаційної безпеки підприємства

Джерело:[складено автором]

Діагностику рівня інформаційної безпеки підприємства пропонується проводити за трьома напрямками (рис. 2.10):

– програмно-технічна захищеність інформації;
– інформаційна надійність співробітників;
– оцінка інформації, що передається керівництву для прийняття рішення.



Рис.2.10. Визначення стану інформаційної безпеки підприємства

Джерело:[54]

Для оцінки інформаційної надійності персоналу пропонується розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства та коефіцієнт підготовленості персоналу до розпізнавання загроз.

Оцінку інформації, що передається керівництву компанії (які приймають рішення), пропонуємо проводити за допомогою трьох показників: повноти інформації, точності інформації та суперечливості інформації. Ці показники слід доповнювати оцінкою своєчасності отримання інформації та рівнем надійності інформації [59].

Експерти, які залучаються для оцінки загроз, у тому числі й інформаційної, повинні: отримувати доступ до всієї наявної у розпорядженні керівництва агропідприємства інформації; володіти креативним мисленням та відповідними знаннями; бути вільним від особистого зацікавлення у результатах проекту (не лобіювати його).

Можна виділити такі основні методи експертних оцінок, що використовуються для аналізу небезпеки: опитувальники; SWOT-аналіз; троянда та спіраль ризиків; оцінка ризик стадії проекту.

Інформація може існувати в різних формах. Її можна друкувати або писати на папері, зберігати на електронних носіях, пересилати по традиційному або електронною поштою, показувати у фільмах або передавати в усній розмові. Якої б форми не приймає інформація, і які б засоби не використовувалися для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень її захисту.

На сьогоднішній день в ТОВ «МХП-Урожайна країна» рівень використання інформаційних технологій знаходиться на невисокому рівні. Тож і рівень інформаційної безпеки є йому відповідним. На підприємстві використовуються найпростіші програми бухгалтерського обліку «1С: Бухгалтерія». Треба зауважити, що через російську агресію в Україні даний комплекс програмного забезпечення не має офіційних оновлень. Що несе значну загрозу інформаційній безпеці та є, фактично, фінансуванням ворога.

Структура інформаційної безпеки на підприємстві досить давно вже не оновлювалась.

Для захисту від зовнішніх загроз використовується сертифікований український антивірусний продукт «Зілля». Зараз він не відповідає вимогам часу та рекомендаціям регулятора, але цікавий як приклад впровадження системи інформаційної безпеки на підприємстві. Відкриті джерела показують, що розробка системи йшла за загальними принципами, без впровадження унікальних технологій. Складністю при реалізації програми виявилася розгалужена мережа контактів підприємства та клієнтів, що

створює потенційну вразливість при атаці на канали зв'язку.

Безумовно, всім доведеться вчитися жити в умовах, коли підприємствам будь-якого розміру в будь-якій країні світу регулярно доведеться стикатися з інцидентами інформаційної безпеки.

Так, в Україні цей показник має неухильну тенденцію до збільшення та, більше того, вже наближається до 100%. 98% підприємств за минулий рік зіткнулися з інцидентом інформаційної безпеки, який був викликаний дією зовнішнього чинника. Також за цей період зросла кількість підприємств, що зазнали зовнішніх атак. Протягом кількох років найзначнішою загрозою спеціалісти називають шкідливе ПЗ, практично не відстає від нього спам, який часто є носієм шкідливого ПЗ. Збільшилася частка тих, хто зіткнувся з фішинговими атаками. Спостерігається і серйозне зростання кількості відмов в обслуговуванні, зросла частка корпоративного шпигунства. Це переважно стосується великих підприємств. По всіх інших пунктам зовнішні загрози також демонструють тенденцію до зростання.

Згідно зі статистичними даними число інцидентів у галузі інформаційної безпеки щороку зростає. Зростання числа інцидентів паралельно зі збільшенням обсягів даних, що передаються в електронному форматі, призводить нас до очевидного висновку: рівень втрат інформації стає все вищим. Цього року під час опитування 24% респондентів повідомили про втрату даних внаслідок інцидентів у галузі інформаційної безпеки, що на 16% більше, ніж у 2022 р.

Цілком логічним видається те, що у міру збільшення кількості інцидентів у сфері безпеки зростатимуть і фінансові втрати. Так і відбувається практично. Подальший аналіз отриманих даних показав, що найбільш суттєве зростання фінансових витрат відзначено в компаніях респондентів, які повідомили про збитки на великі суми внаслідок інцидентів у сфері безпеки.

Впровадження політики та необхідних регламентів, а також залучення топ-менеджменту в роботу над удосконаленням систем безпеки стає

початком реальної діяльності. Ефективність вжитих заходів можна оцінити, проаналізувавши застосування компаніями технологій, які забезпечують впровадження такої політики та регламентів.

Одним із прикладів ефективних заходів безпеки є інформування співробітників та організація навчання персоналу. Інформованість працівників є дуже важливим чинником будь-якої програми безпеки. 60% опитаних кажуть, що у їхніх компаніях є навчальні програми, призначені підвищення рівня поінформованості співробітників.

Особлива увага приділяється таким п'яти категоріям захисних заходів, як захист важливих активів, забезпечення безпеки інфраструктури, виявлення загроз безпеки, аналітичні заходи та забезпечення безпеки мобільних пристроїв. Нажаль, в ТОВ «МХП-Урожайна країна» відсутня структура, що відповідає за це напрямок безпеки.

Для того, щоб підвищити надійність інфраструктури, практично 1/4 опитаних співробітників підприємства (24%) планують запровадити стандарти безпеки для зовнішніх партнерів, постачальників та клієнтів. Це завдання стає все більш актуальним у міру того, як компанії відкривають доступ до своїх мереж, додатків та даних для третіх осіб. Більше того, застосування таких технологій, як віртуалізація та хмарні обчислення, що істотно підвищило ймовірність загроз, які можуть виходити від інсайдерів, які мають високі повноваження доступу. Таким чином, моніторинг і управління користувачами з високим рівнем доступу тепер входять до основних проблем. Дослідження показало, що 17% опитаних планують запровадити інструменти для керування користувачами з високим рівнем доступу протягом наступних 12 місяців [46].

З урахуванням дедалі більшого інтересу до методів обробки великих масивів інформації було включено питання про плани компаній щодо застосування аналітичних схем з метою підвищення загальної безпеки. Стратегічний підхід до цього питання стає дедалі популярнішим: 20% респондентів сказали, що планують у майбутньому переглянути

пріоритетність інструментів інформаційної безпеки та управління подіями. Стільки ж опитаних вважають запровадження технологій кореляції подій у системах захисту своїм першочерговим завданням.

Минулий рік показав, що обмін інформацією про загрози безпеці, навіть між конкуруючими компаніями, став потужним інструментом протидії ризикам.

ТОВ «МХП-Урожайна країна» - підприємство Сумської області, що займається вирощуванням сільськогосподарської продукції.

Компанія обробляє понад 32 000 гектарів землі в Сумській області. Він вирощує зернові та промислові культури, переважно пшеницю, ріпак, кукурудзу, соняшник, горох та сою. У 2021 році на території компанії було зібрано понад 184000 тонн зерна. ТОВ «МХП-Урожайна країна» створено в 2010 році. Компанія входить в агропромислову структуру МХП. І здійснює діяльність на території Сумської області. У 2015 році-увійшло до рейтингу найприбутковіших сільськогосподарських підприємств з вирощування зернових культур.

ТОВ «МХП-Урожайна країна» входить в агропромислову структуру МХП. Компанія МХП є великим гравцем на аграрному ринку, виробничі потужності якого охоплюють 12 областей України. Земельний банк становить 360 000 га, з них під вирощування сільськогосподарських культур – 353 000 га. МХП також є одним з найбільших роботодавців в країні, де сьогодні працює більше 32 тисяч людей.

У 2021 р. капітал ТОВ «МХП-Урожайна країна» збільшився на 840651 тис.грн, або на 35,18 %. Це відбулося в основному за рахунок збільшення позикового капіталу на 613498 тис.грн, або більш ніж в 1,37 рази, що складається в основному з короткострокового капіталу. У 2020-2022 роках довгострокові капітальні позики не видавалися. Обсяг капіталу збільшився на 227153 тис.грн. за рахунок збільшення нерозподіленого прибутку на 9,52 % у 2021 році, а оборотний капітал залишився незмінним. Чистий дохід у 2021 році зріс майже в 2 рази порівняно з 2020 роком, але дещо знизився у 2022

році, знизившись на 10,76% порівняно з попереднім роком. Так, у 2021 році порівняно з 2020 роком собівартість продукції значно зросла на 74,64%, або на 463957 тис.грн. У 2022 році собівартість знизилася такими ж темпами, як і чистий дохід - вона знизилася на 13,88%, або на 150626 тис.грн.

Інформаційна безпека будь-якого підприємства демонструється завдяки захищеності його інформаційного середовища та ефективності інформаційного забезпечення всього процесу управління підприємством.

Для оцінки інформаційної надійності персоналу пропонується розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства та коефіцієнт підготовленості персоналу до розпізнавання загроз.

Особлива увага приділяється таким п'яти категоріям захисних заходів, як захист важливих активів, забезпечення безпеки інфраструктури, виявлення загроз безпеки, аналітичні заходи та забезпечення безпеки мобільних пристроїв.

РОЗДІЛ 3
ПРОЕКТ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ НА ПРИКЛАДІ ТОВ «МХП-УРОЖАЙНА КРАЇНА»

3.1. Методи забезпечення інформаційної безпеки агропромислових підприємств

Найпростіший приклад заходу з інформаційної безпеки – антивірус, встановлений на комп'ютері. Але в комерційних структурах до цього питання підходять серйозніше і на багатьох рівнях, щоб забезпечити безпеку, потрібно зробити значно більше ніж елементарне встановлення антивірусних програм.

Засоби інформаційної безпеки захищають дані від витоку, програми, системи та мережі – від злому, несанкціонованого доступу, псування файлів чи інших видів атак. Якщо йдеться про комерційні чи державні структури, відомості також захищають від шпигунів чи можливих зловмисників усередині самого колективу.

Інформаційна безпека захищає системи від проникнення та від атак. Сюди входить не тільки злом: це і DDoS-атаки, внаслідок яких може «лягти» сервер сайту, і витік даних, і багато іншого. Зловмисників набагато більше, ніж здається. І ніхто не хоче, щоб їх сервіс втратив працездатність, а дані виявились доступними всім навколо. Для цього потрібна інформаційна безпека.

У компаній є ще одна причина: за витік конфіденційних даних користувачів вони несуть відповідальність за законом. Тож для них заходи щодо безпеки - це ще й спосіб уникнути проблем із законодавством та втрати довіри клієнтів.

Без заходів з інформаційної безпеки будь-хто міг би отримати доступ до конфіденційних відомостей або зламати будь-який сайт чи систему

комп'ютерним простором стало б практично неможливо скористатися. Діюча сьогодні методика захисту інформації складаються з трьох напрямків: організаційно-технічного, правового та економічного.

Організаційно-технічний напрямок інформаційної безпеки включає в себе:

- розгалужену та дієву систему інформаційної безпеки яка складається з комплексу заходів та технічних засобів. Що мають на меті збереження конфіденційності даних;
- розробка, створення нових та використання усіх доступних засобів захисту інформації;
- постійний контроль за результатами проведених заходів у сфері захисту конфіденційної та бізнесової інформації.

Без якісної та сталої системи оцінювання результатів проведених заходів фактично неможливо визначити їх ефективність. Якщо їх ефективність знижується, потрібні термінові корективи (адже це і є завданням постійного контролю).

Організаційно-технічний напрямок тісно пов'язаний з правовим напрямком інформаційної безпеки.

Правовий напрямок інформаційної безпеки складається з наступних обов’язкових умов:

- отримання ліцензії на діяльність пов’язану з забезпеченням інформаційного захисту;
- отримання та підтвердження сертифікатів на технічні засоби захисту;
- атестація об'єктів інформатизації відповідно до встановлених правил інформаційного захисту.

Економічна складова захисту інформації включає в себе:

- створення та використання програм та заходів з метою дотримання інформаційної безпеки;

- виділення необхідного фінансового забезпечення для виконання цих заходів;
- впровадження механізмів страхування ризиків інформаційної безпеки [22].

Інформаційна безпека завжди була складною системою, всі її компоненти спрямовані на запобігання втраті інформації. Втрата конфіденційної інформації за допомогою технічних засобів та унеможливлення доступу до носіїв інформації сторонніх осіб – головна спонукальна причина розвитку технічних засобів захисту.

Технічними засобами підприємства можна визначити використання спеціальних електронних пристроїв. Пристрої для протидії несанкціонованому вилученню інформації як в приміщеннях, так і в комунікаціях.

В Україні існують різноманітні нормативно-правові документи, які регламентують роботу в наступних сферах: інформаційний простір: «Про затвердження Доктрини інформаційної безпеки України»; «Про захист інформації, інформаційні технології та інформацію» та ін. Одним з базових є «Закон України про комерційну таємницю». До цього переліку мають увійти і рішення українського уряду «Про сертифікацію засобів захисту інформації» та «Про ліцензування засобів технічного захисту та конфіденційну інформацію». [55].

З точки зору економічної складової інформаційної безпеки, то найважливішим правилом є те, що вартість усієї структури інформаційного захисту не повинна перевищувати вартості тієї інформації, що захищається. Захищати потрібно конкретну інформацію, а не весь потік інформації, що економічно недоцільно.

Щоб визначити активи, які потрібно захистити, їх компоненти потрібно розібрати. Ці компоненти є наступними:

- аудіо інформація;
- інформація, що передається за допомогою технічних засобів [50].

Технічні засоби та обладнання, інструменти та пристрої, що використовуються на підприємстві, а також усі супутні приміщення повинні бути захищені.

Захист корпоративної інформації полягає у встановленні та дотриманні певних правил, розроблених з урахуванням законодавства України. Його завдання — запобігати несанкціонованому доступу до конфіденційних даних.

Організаційні методи забезпечення інформаційної безпеки такі:

- системи захисту інформації;
- правила взаємовідносин між працівниками;
- постійні правила роботи з документами;
- правила користування окремими технічними засобами;
- аналітична робота з оцінки загроз інформаційній безпеці [53].

Інформаційні компоненти захищені від несанкціонованого доступу співробітників компанії шляхом обмеження доступу до носіїв інформації та каналів їх передачі. Цей спосіб не вимагає великого використання технічних засобів.

До технічних способів забезпечення захисту інформації відносяться технічні елементи системи захисту інформації та використання різноманітних програм для забезпечення інформаційної безпеки. До них відносяться: системи управління базами даних, прикладне ПЗ, різні засоби шифрування, системи DLP і SIEM для запобігання втраті даних у комп’ютерних мережах тощо.

Організаційно-технічні методи повинні діяти виключно в межах правового поля забезпечення інформаційної безпеки, передбачених чинним законодавством України.

Структура інформаційної безпеки створюється з урахуванням багатьох підсистем. До них відносяться наступні:

- підсистема доступу до інформації;

- підсистема реєстрації та контролю інформації;
- підсистема безпеки з використанням шифрів;

Головними правилами якісної системи інформаційної безпеки вважаються:

- постійність заходів для захисту даних, відповідно встановлених правил;
- повнота та доцільність запропонованих мір;
- комплексність;
- результативність.

Методи захисту аудіо інформації.

Для забезпечення захисту аудіо інформації потрібно чітко встановити розміри території, які вимагають охорони, обмежити допуск співробітників на визначену територію.

Для збільшення інформаційної безпеки можна використовувати вібро- та аудіоізоляцію, екранування та автономізацію засобів передачі інформації.

За можливості необхідно використовувати різноманітні активні та пасивні засоби аудіо безпеки. До активних відносимо електромагнітні генератори, за допомогою яких виробляються «білий шум», що перешкоджає технічному втручанню в інформаційні потоки. До пасивних: вібро- та звукоізоляція; екрануючі пристрої; звукопоглинаючі фільтри та інше.

Для забезпечення захисту інформації, що зберігається та передається технічними засобами, в Україні використовують:

- різноманітні види автентифікації;
- обмеження доступу до об'єктів;
- шифрувальні системи;
- ключі;
- безпечні та виділені по'єднання з мережею інтернет;
- IPsec [7].

Розглянемо кожну з цих форм захисту інформації детальніше.

Такі елементи захисту інформації, як логіни та паролі, є обов’язковими для всіх хто має доступ до операційної системи. Це найпоширеніший спосіб забезпечення мінімального рівня безпеки даних, у тому числі інформаційних повідомлень, що зберігаються на серверах і пристроях.

Обмеження доступу до об'єктів, що потребують охорони також можливе за допомогою аутентифікації, але вимагає додаткових заходів захисту. Наприклад, права доступу можуть бути обмежені залежно від завдання або обмеження прав на копіювання, зміни чи видалення інформації.

Файли зашифровані ключем не є фіксованим методом захисту і змінюється через нерегулярні проміжки часу.

Захищені з'єднання встановлюються через спеціальні інформаційні канали "клієнт-клієнт" або "клієнт-сервер". В Україні цей метод захисту інформації використовується насамперед у банківській сфері.

Автоматизація бізнес-процесів у компанії – нагальна вимога їх подальшого існування. У сучасних умовах відсутність швидкої реакції і гнучкості внутрішніх процесів підприємства призводить до його банкрутства. В той же час автоматизація процесів прискорює рух виробленого товару, перетворює роботу кожного співробітника на комфортною та, забезпечує безпеку фірми. Проте інформаційна безпека при автоматизації бізнесу зазнає значних змін.

Отже необхідно враховувати наступні проблеми:

Помилки при налаштуванні програм можуть бути спричиненими шахрайством з боку несумлінних робітників. Погано об лаштовану та не захищену систему можуть ззовні атакувати хакери і викрасти кошти, або бізнесову інформацію.

Компанія, що використовує автоматизацію у своїй діяльності, може навмисно або випадково отримати доступ до інформації, якої у них не повинно бути. Як згодом вони розпорядяться ними – питання відкрите.

Під поняттям програм для автоматизації існує цілий комплекс різного

за архітектурою та призначенням програмного забезпечення, який розроблено для вирішення різноманітних завдань для бізнесу.

Інформаційна безпека автоматизованих систем управління (АСУ) забезпечується здатністю цієї системи зберігати конфіденційність інформації при її введенні, виведенні, передачі, обробці та зберіганні, а також протистояти її руйнуванню, розкраданню чи спотворенню. Об'єктом захисту в АСУ є дані, що містять конфіденційні (секретні) відомості, що зберігаються, обробляються та передаються між елементами автоматизованої системи управління.

Підходи до забезпечення інформаційної безпеки АСУ відрізняються від забезпечення безпеки інформаційно-обчислювальних систем загалом через низку особливостей їх реалізації та експлуатації:

- управління технічно складними життєво важливими об'єктами;
- робота в режимі реального часу;
- критичність до часу реакції системи;
- великий час життєвого циклу системи;
- територіальна розподіленість [74].

Відсутність єдиної технології проектування та модернізації та універсальної елементної основи.

Раніше ймовірність таких інцидентів, як зараження програмного забезпечення компонентів АСУ шкідливими програмами Stuxnet, Duqu або Flame, вважалася невеликою. Причиною цього були принципи, які застосовувалися при побудові АСУ: закрите програмне забезпечення, протоколи та технології, фізична ізоляція.

Дані принципи робили важкодоступною та малоефективною атаку на автоматизовані системи та промислові об'єкти автоматизації.

Однак зміни в апаратному та програмному забезпеченні сучасних АСУ призвели до виникнення нових видів уразливості, які не можуть бути ліквідовані існуючими підходами щодо забезпечення інформаційної безпеки. Крім того, метою атаки на промислові об'єкти можуть бути не лише

руйнація, а й політичний тиск [27].

Нижче наведено основні зміни в елементній базі та архітектурі АСУ, що спричинили появу нових уразливостей у системі інформаційної безпеки:

- Впровадження відкритих мережевих комунікаційних протоколів;

- Збільшення потужності обчислювальних пристроїв (прикладом можуть бути програмовані логічні контролери, ПЛК);

- Взаємодія компонентів розподілених систем через мережу, зокрема Інтернет;

- Інтеграція з корпоративними мережами та інформаційними системами [34].

Ускладнює завдання забезпечення безпеки в цілому те, що зміни можуть охоплювати не всю систему, а лише її окремі модулі. З одного боку, полегшує зловмисникам доступ до АСУ мереж наявність доступних для публічного перегляду прикладів використання існуючих вразливостей. З іншого боку, зміни породили нові способи отримання вигоди: здирництво та нецільове використання обчислювальних потужностей.

Але за логікою процесу, саме автоматизовані системи управління виробничими процесами мають найменшу кількість вразливостей, адже вони зациклені самі на собі та в меншій мірі потребують доступу до зовнішньої інформації. Також АСУ побудовані в одній архітектурі, тож пошук і ліквідація вразливостей значно спрощене. Адже програмне забезпечення має спільну базу. Окрім цього впровадження таких систем забезпечить:

– Оптимізацію керування технологічними процесами.

– Підвищення конкурентоспроможності продукції, за рахунок підвищення її якості.

– Зниження собівартості, що досягається з допомогою мінімізації витрат за виробництво.

На даному етапі розвитку світової економіки рівень комп'ютеризації суспільства та бізнесу має вирішальне значення. Є потреба в активному застосовувані цифрових технології. Таким чином, двигуном інновацій,

конкурентоспроможності та економічного розвитку країни є цифрова економіка.

Європейські країни намагаються забезпечити нові можливості для підприємств та прискорити «цифрові» трансформації свого бізнес-ландшафту. З цією метою прийняті рішення про стимулювання використання новітніх цифрових технологій, які вдосконалюють бізнес-процеси, створюють нові бізнес-моделі, удосконалюють бізнес-аналітику взаємодії з клієнтами, підвищення темпів зростання та створення робочих місць.

У 2018 році Уряд затвердив Концепцію розвитку цифрової економіки та суспільства України.

Автоматизація окремих процесів, та комплексна автоматизація всього виробництва із застосуванням автоматизованих систем управління - одне з основних напрямів науково-технічного прогресу у сфері сільського господарства. Для оптимального управління сільським господарством у масштабі усієї галузі в Україні потрібна галузева автоматизована система управління.

3.2. Пропозиції щодо удосконалення основних напрямів підвищення ефективності роботи та інформаційної безпеки ТОВ «МХП-Урожайна країна»

Сьогодні повністю захистити промислову компанію, або будь-яку іншу компанію, від злому і проникнення в мережу практично неможливо. Тому бізнес на рівні топ-менеджменту та ключових осіб заговорив про необхідність отримання результату на іншому рівні. У наукових колах це називається концепцією ефективної кібербезпеки, яка, в свою чергу, включає в себе концепцію неприпустимих подій.

Ефективна безпека – це якісно та кількісно вимірювана система захисту інформації, яка забезпечує збереження важливих для компанії активів та запобігає виникненню неприпустимих подій.

Завжди є події, неприпустимі для підприємства. Щоб такі події не відбулися, необхідно чітко визначити їх, а також їх можливі наслідки. Також необхідно забезпечити такий рівень інформаційної безпеки, який виключає настання неприпустимих подій в результаті кібератаки. Підхід ефективної кібербезпеки вже почав застосовуватися в українських компаніях. Його мета – кардинально підвищити безпеку компаній, а через них – захист галузей промисловості та країни в цілому.

Неприпустима подія – це подія, яка відбувається в результаті дій зловмисників і унеможливлює досягнення компанією своїх операційних і стратегічних цілей або призводить до довгострокового порушення її основної діяльності.

В даний час кібербезпека на підприємствах в більшості випадків будується за одним досить простим принципом: кожен фахівець виконує свої функції строго в межах своєї відповідальності, відповідно до своєї посадової інструкції і власним регламентом роботи.

Наприклад, припустимо, є промисловий об'єкт з системами управління технологічними режимами, обладнанням і процесами. З їх допомогою диспетчер контролює виробництво і контролює його. Але він не бачить, що відбувається в IT-інфраструктурі об'єкта, і не знає, які критичні події в IT-системах можуть спричинити проблеми на технологічному рівні. Це не його службовий обов'язок, не його функціональне завдання.

Водночас, враховуючи важливість безперервної роботи критичних об'єктів та необхідність їх захисту від кібератак та внутрішніх зловмисників, підприємства, безумовно, впроваджують системи кібербезпеки. Так, на об'єкті з'являється ще один фахівець — співробітник служби безпеки, який стежить за всіма подіями, що відбуваються в IT-інфраструктурі об'єкта або підприємства в цілому. Цікаво, що робить він це у відриві від основної діяльності об'єкта і не має ні найменшого уявлення про те, як функціонує підприємство, які режими роботи основного обладнання або виробничих ліній вважаються аварійними. А також порогові значення потужності або

частоти і що означає перевищення цих значень.

Причина та сама – це не його зона функціональної відповідальності і не посадовий обов'язок [65].

В результаті ні диспетчер, ні співробітник служби безпеки не бачать всієї картини функціонування підприємства.

Інформатизація як послідовність розвитку необхідна нашій країні. Вона є невід'ємною умовою для вирішення завдань його вдосконалення [3]. Розвиток АПК - одне з найважливіших завдань, пов'язана з динамічним впровадженням сучасних технологій, застосуванням останніх досягнень науки і техніки. Для підвищення ефективності агропромислового комплексу необхідно вдосконалювати систему управління як кожному окремо взятому підприємстві, а й у рівні галузей і АПК загалом, впроваджувати сучасні інформаційні технології [46]. Застосування високих технологій для вдосконалення АПК України дозволить результативно і в короткий період:

– ввести нові технології в землеробство і тваринництво;

– обладнати АПК сучасною технікою; досягти заощадження фінансових коштів бюджетів усіх рівнів;

– посилити координованість господарства.

Тому використання інформаційних технологій в агропромисловому виробництві повинно не просто описувати сформовану ситуацію, але і давати рекомендації щодо перетворення організації та управління для досягнення більш високих результатів [46].

Такою технологією можна вважати новітню програму “BAS АГРО. ERP”. Це комплексна інформаційна система експертного класу, що дозволяє автоматизувати управління діяльністю середніх і великих сільськогосподарських підприємств різних організаційно-правових форм. Рішення підходить для агрохолдингів з рослинництвом, агропромислових виробництв, великих зернових трейдерів.

Програмний продукт "BAS АГРО. ERP" є розробкою черкаської компанії CONTO, та має призначення автоматизувати управління діяльністю

агропідприємств різних форм власності та організації.

Програмне забезпечення "BAS АГРО. ERP" розроблено на базі основного продукту компанії та містить весь функціонал продукту, та автоматизує наступну галузеву специфіку рослинництва (Рис. 3.1.):



Рис. 3.1. Функціональні складові "BAS АГРО. ERP"

Джерело:[розроблено автором]

Це рішення забезпечує автоматизацію всіх ключових бізнес-процесів в організації управління компанією та забезпечує автоматизацію бізнес-процесів у виробництві продукції та інших супутніх товарів і послуг.

Програма передбачає впровадження автоматизованих робочих місць для кожного окремого процесу. Це дозволяє швидко та зручно опрацьовувати інформацію та отримувати аналітичні звіти з різних напрямків роботи агропромислових підприємств.

Автоматизоване робоче місце (АРМ) «Управління транспортом» дозволяє не тільки реєструвати окремі транспортні дані, а й демонструє наявну довжину транспортної черги та вказує, які пункти пропуску позначені для того чи іншого виду транспорту чи транспортного засобу. Функції безпеки в цій частині програми дозволяють контролювати та записувати дозволи на в’їзд та виїзд для кожного транспортного засобу.

АРМ «Лабораторія» веде реєстрацію результатів аналізів різної сільськогосподарської продукції, визначає та відмічає відповідність встановленим на підприємстві стандартам якості. У разі потреби тут же визначають чергу, ремонт і доступ до лабораторії машин та механізмів, необхідних для технічної роботи з зерном.

Робоча зона «Вагова» координує всю зону зважування. Дані отримуються автоматично або вручну з ваг і проводяться розрахунки ваги, знижок і надбавок (визначених компанією). Програма самостійно визначає спосіб прийому або відвантаження продукції. Також передбачено комплексний кількісний та якісний облік продукції та автоматичне завантаження необхідних даних перед початком роботи. Послідовний кількісний і якісний облік веде до детальної операційної звітності для аналізу та виправлення.

АРМ «Підробіток зерна» створене для формування та виконання виробничих операцій з продуктами виробництва та створення відповідних фінансових документів. Після обробки визначеного обсягу продукції вираховується собівартість послуг зберігання продукції.

В комп’ютерній програмі передбачено та реалізовано зручний механізм створення технологічних карт полів з можливістю їх актуалізації відповідно до періодів вирощування. Також механізми системи дозволять отримувати детальну аналітику в розрізі культур, полів і видів робіт та витрат на їх вирощування та обробку. Звітність про отримані результати та аналіз подається в будь-якому зручному графічному вигляді.

Робоче місце «Склад» забезпечує доступність, оцінку вартості і розрахунки місця для зберігання для більшості компонентів бюджету:

- засоби захисту рослин, насіння та добрива;
- паливно-мастильні матеріали;
- орендовані/власні землі;
- транспортна амортизація;
- матеріальне заохочення усіх видів та відрахування;

- продажі.

Автоматична організація видаткових бюджетів планується на основі підготовлених планових даних. Вартісна організація прямих і непрямих витрат планується як по окремих культурах, так і по розрізу полів.

Підсумковий звіт «Інформація про сільськогосподарські витрати» містить детальний аналіз фактичних витрат, пов’язаних з полями, посівами чи різними видами робіт.

У ньому передбачені розрахунки та розрахунки існуючих пенсій двома способами: у фіксованому розмірі або у відсотках. Це також дозволяє врахувати інфляцію та розрахувати майбутню орендну плату. Крім того, акціонери можуть вибирати між різними видами орендної плати, як у формі грошей, так і у формі виробничих благ (зерна, послуг та інших негрошових засобів). Крім того, рента може обчислюватися і сплачуватися частково грошима, а частково — виробленими товарами та послугами.

Програмою передбачений автоматичний звіт "Відомості про наявність земельних ділянок" який використовується як додаток до Декларації платника єдиного податку четвертої групи і регламентованого звіту "форма № 1ДФ".

Програмне забезпечення «BAS АГРО. ERP» має відкриту архітектуру, це забезпечує можливість її поєднання з корпоративними системами супутникового моніторингу обробляємих земель, та іншими системами управління документообігом. Тобто до неї без проблем можна підключити бази інших програм. Які використовувалися раніш: як професійних сільськогосподарських, так і бухгалтерських.

"BAS АГРО. ERP» - це програмне рішення, метою якого є автоматизація управління бізнес-процесами середніх та великих підприємств, що займаються сільськогосподарською діяльністю.

Конфігурація "BAS АГРО. ERP" задовольняє потреби в автоматизації діяльності та управління аграрних організацій таких напрямків як виробництво продуктів рослинництва, супутніх товарів чи надання послуг.

Програмний продукт "BAS АГРО. ERP" має широкий функціональний апарат який дозволяє не тільки планувати сільськогосподарське виробництво, а і забезпечує оперативний облік сіль господарських робіт та послуг та вираховує озрахункі з пайовиками.

Програмне рішення "BAS АГРО. ERP" поставляється в електронному форматі, в який входять усі необхідні програмні компоненти, нормативна документація, набір пін-кодів, реєстраційні та користувацькі угоди.

Придбати продукт "BAS АГРО. ERP" можна у вигляді основного постачання та додатково придбати користувацькі та серверні ліцензії на необхідну кількість робочих місць.

Також можна оформити замовлення на постачання "BAS АГРО. ERP" на умовах заміни або доопрацювання вже чинної конфігурації.

Право на придбання цього програмного рішення за умовами апгрейду мають власники таких прикладних рішень:

– усі версії продуктів платформи 1С:Підприємство 7.7;

– конфігурації 1С:Підприємство 8:

– бухгалтерія;

– бухгалтерія сільськогосподарського підприємства;

– бухгалтерія елеватора, млина та комбікормового заводу;

– управління торгівлею;

– зарплата та Управління персоналом;

– управління невеликою фірмою;

– управління торговим підприємством;

– управління виробничим підприємством;

– управління сільськогосподарським підприємством;

– рішення для бюджетної сфери;

– всі версії технологічних поставок.

Крім того, фірма Конто пропонує власні продукти, що є додатковими до базового продукту BAS:

– BAS Бухгалтерія (професійний);

– BAS Бухгалтерія (корпоративний);

– BAS Управління торгівлею;

– BAS Комплексне управління підприємством.

На умовах апгрейду можливе придбання ліцензій для програмного продукту. Актуальним це для користувачів, які працюють у таких конфігураціях:

– бухгалтерія сільськогосподарського підприємства;

– управління сільськогосподарським підприємством;

– бухгалтерія елеватора, млина та комбікормового заводу.

Вартість продукту залежить від потужностей підприємства та кількості робочих місць. Оптимальний підбор допоможуть розрахувати спеціалісти компанії.

Для забезпечення високої продуктивності та забезпечення інформаційної безпеки в ТОВ «МХП-Урожайна країна» рекомендуємо використовувати загальне програмне забезпечення на кшталт "BAS АГРО. ERP".

Засоби інформаційної безпеки захищають дані від витоку, програми, системи та мережі - від злому, несанкціонованого доступу, псування файлів чи інших видів атак. Якщо йдеться про комерційні чи державні структури, відомості також захищають від шпигунів чи можливих зловмисників усередині самого колективу.

Розвиток АПК - одне з найважливіших завдань, пов'язана з динамічним впровадженням сучасних технологій, застосуванням останніх досягнень науки і техніки. Для підвищення ефективності агропромислового комплексу необхідно вдосконалювати систему управління як кожному окремо взятому підприємстві, а й у рівні галузей і АПК загалом, впроваджувати сучасні інформаційні технології [4].

Застосування високих технологій для вдосконалення АПК України

дозволить результативно і в короткий період:

- ввести нові технології в землеробство і тваринництво;
- обладнати АПК сучасною технікою; досягти заощадження фінансових коштів бюджетів усіх рівнів;
- посилити координованість господарства.

Тому використання інформаційних технологій в агропромисловому виробництві повинно не просто описувати сформовану ситуацію, але і давати рекомендації щодо перетворення організації та управління для досягнення більш високих результатів.

Автоматизація окремих процесів, та комплексна автоматизація всього виробництва із застосуванням автоматизованих систем управління - одне з основних напрямів науково-технічного прогресу у сфері сільського господарства. Для оптимального управління сільським господарством у масштабі усієї галузі в Україні потрібна галузева автоматизована система управління.

За логікою процесу, саме автоматизовані системи управління виробничими процесами мають найменшу кількість вразливостей, адже вони зациклені самі на собі та в меншій мірі потребують доступу до зовнішньої інформації. Також АСУ побудовані в одній архітектурі, тож пошук і ліквідація вразливостей значно спрощене. Адже програмне забезпечення має спільну базу. Окрім цього впровадження таких систем забезпечить:

Оптимізацію керування технологічними процесами.

Підвищення конкурентоспроможності продукції, за рахунок підвищення її якості.

Зниження собівартості, що досягається з допомогою мінімізації витрат за виробництво.

Для забезпечення високої продуктивності та забезпечення інформаційної безпеки в ТОВ «МХП-Урожайна країна» рекомендуємо використовувати загальне програмне забезпечення на кшталт "BAS АГРО. ERP".

ВИСНОВКИ

У сучасному світі, де інформаційні технології отримують все більш важливу роль у всіх сферах життєдіяльності людини (особливо у бізнесі), гарантія безпеки інформації стає критичною вимогою для сталого розвитку суспільства взагалі та його економічних складових зокрема. Загрози з боку кіберзлочинців, несанкціонований доступ до даних, виток інформації та інші ризики вимагають від компаній ефективного управління інформаційною безпекою.

Інформаційна безпека в компаніях і на підприємствах — це комплекс організаційних і технічних заходів для захисту та безпеки інформації та її основних компонентів, а також пристроїв і систем, які використовуються для обробки, зберігання та передачі інформації. Цей комплекс включає прийоми, норми та методи управління інформацією, що забезпечують ефективний захист інформації.

Забезпечення інформаційної безпеки передбачає захист інформації та інформаційної інфраструктури підприємства від негативних впливів. Ці впливи можуть бути випадковими чи навмисними, внутрішніми чи зовнішніми. В результаті таких втручань важлива інформація може бути втрачена, неавторизовано змінена або використана третіми особами. Таким чином, інформаційна безпека є важливим аспектом корпоративного захисту та безперервності бізнесу.

Заходи захисту інформації визначаються як пристрої, обладнання, програмне забезпечення та організаційні заходи, що запобігають втраті інформації та забезпечують її захист під впливом усіх існуючих загроз.

Для захисту даних у сучасних мережах використовуються різні спеціалізовані програми. Можна виділити такі типи програмних засобів захисту:

• Антивірусне програмне забезпечення.

• Хмарні антивіруси (CloudAV).

• Рішення DLP (Data Leak Prevention).

• Системи криптографії.

• Міжмережеві екрани (МСЕ).

• Віртуальні приватні мережі VPN (Virtual Private Network).

• Проксі-сервер.

• Рішення SIEM – системи моніторингу та управління інформаційною безпекою.

Загрози інформаційної безпеки можна поділити на два типи: природні та штучні. До природних належать природні явища, які залежить від людини, наприклад урагани, повені, пожежі тощо. Штучні загрози залежать безпосередньо від людини і можуть бути навмисними та ненавмисними.

Великі підприємства агропромислового комплексу, як комерційні, так і державні, мають великий досвід забезпечення інформаційної безпеки в умовах обмежених ресурсів. У більшості випадків служби безпеки та охорони займаються цими питаннями окремо.

Однак для малих та середніх підприємств (МСП) такий підхід неможливий через їхні розміри та витрати. Керівництво таких підприємств вважає за краще економити на заходах інформаційної безпеки, що може призвести до значних фінансових і моральних втрат і навіть руйнування бізнесу.

З огляду на вищезазначене, розробка та вдосконалення інструментарію та методичного інструментарію оцінки інформаційної безпеки та впровадження заходів інформаційної безпеки на підприємствах агропромислового комплексу є актуальним питанням.

ТОВ «МХП-Урожайна країна» - підприємство Сумської області, що займається вирощуванням сільськогосподарської продукції.

Компанія обробляє понад 32 000 гектарів землі в Сумській області. Він вирощує зернові та промислові культури, переважно пшеницю, ріпак, кукурудзу, соняшник, горох та сою. У 2021 році на території компанії було зібрано понад 184000 тонн зерна. ТОВ «МХП-Урожайна країна» створено в

2010 році. Компанія входить в агропромислову структуру МХП. І здійснює діяльність на території Сумської області. У 2015 році-увійшло до рейтингу найприбутковіших сільськогосподарських підприємств з вирощування зернових культур.

ТОВ «МХП-Урожайна країна» входить в агропромислову структуру МХП. Компанія МХП є великим гравцем на аграрному ринку, виробничі потужності якого охоплюють 12 областей України. Земельний банк становить 360 000 га, з них під вирощування сільськогосподарських культур – 353 000 га. МХП також є одним з найбільших роботодавців в країні, де сьогодні працює більше 32 тисяч людей.

У 2021 р. капітал ТОВ «МХП-Урожайна країна» збільшився на 840651 тис.грн, або на 35,18 %. Це відбулося в основному за рахунок збільшення позикового капіталу на 613498 тис.грн, або більш ніж в 1,37 рази, що складається в основному з короткострокового капіталу. У 2020-2022 роках довгострокові капітальні позики не видавалися. Обсяг капіталу збільшився на 227153 тис.грн. за рахунок збільшення нерозподіленого прибутку на 9,52 % у 2021 році, а оборотний капітал залишився незмінним. Чистий дохід у 2021 році зріс майже в 2 рази порівняно з 2020 роком, але дещо знизився у 2022 році, знизившись на 10,76% порівняно з попереднім роком. Так, у 2021 році порівняно з 2020 роком собівартість продукції значно зросла на 74,64%, або на 463957 тис.грн. У 2022 році собівартість знизилася такими ж темпами, як і чистий дохід - вона знизилася на 13,88%, або на 150626 тис.грн.

Інформаційна безпека будь-якого підприємства демонструється завдяки захищеності його інформаційного середовища та ефективності інформаційного забезпечення всього процесу управління підприємством.

Для оцінки інформаційної надійності персоналу пропонується розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства та коефіцієнт підготовленості персоналу до

розпізнавання загроз.

Особлива увага приділяється таким п'яти категоріям захисних заходів, як захист важливих активів, забезпечення безпеки інфраструктури, виявлення загроз безпеки, аналітичні заходи та забезпечення безпеки мобільних пристроїв. Нажаль, в ТОВ «МХП-Урожайна країна» відсутня структура, що відповідає за це напрямок безпеки.

Засоби інформаційної безпеки захищають дані від витоку, програми, системи та мережі — від злому, несанкціонованого доступу, псування файлів чи інших видів атак. Якщо йдеться про комерційні чи державні структури, відомості також захищають від шпигунів чи можливих зловмисників усередині самого колективу.

Розвиток АПК - одне з найважливіших завдань, пов'язана з динамічним впровадженням сучасних технологій, застосуванням останніх досягнень науки і техніки. Для підвищення ефективності агропромислового комплексу необхідно вдосконалювати систему управління як кожному окремо взятому підприємстві, а й у рівні галузей і АПК загалом, впроваджувати сучасні інформаційні технології. Застосування високих технологій для вдосконалення АПК України дозволить результативно і в короткий період:

– ввести нові технології в землеробство і тваринництво;
– обладнати АПК сучасною технікою; досягти заощадження фінансових коштів бюджетів усіх рівнів;
– посилити координованість господарства.

Тому використання інформаційних технологій в агропромисловому виробництві повинно не просто описувати сформовану ситуацію, але і давати рекомендації щодо перетворення організації та управління для досягнення більш високих результатів.

Автоматизація окремих процесів, та комплексна автоматизація всього виробництва із застосуванням автоматизованих систем управління - одне з основних напрямів науково-технічного прогресу у сфері сільського

господарства. Для оптимального управління сільським господарством у масштабі усієї галузі в Україні потрібна галузева автоматизована система управління.

За логікою процесу, саме автоматизовані системи управління виробничими процесами мають найменшу кількість вразливостей, адже вони зациклені самі на собі та в меншій мірі потребують доступу до зовнішньої інформації. Також АСУ побудовані в одній архітектурі, тож пошук і ліквідація вразливостей значно спрощене. Адже програмне забезпечення має спільну базу. Окрім цього впровадження таких систем забезпечить:

- Оптимізацію керування технологічними процесами.
- Підвищення конкурентоспроможності продукції, за рахунок підвищення її якості.
- Зниження собівартості, що досягається з допомогою мінімізації витрат за виробництво.

Для забезпечення високої продуктивності та забезпечення інформаційної безпеки в ТОВ «МХП-Урожайна країна» рекомендуємо використовувати загальне програмне забезпечення на кшталт "BAS АГРО. ERP".

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 251 -253 с.

2. Андреєва Н. М., Бараннік В. О., Бєлашов Є. В. та ін. Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях. За науковою ред. д. екон. н., проф. Хлобистова Є. В. РВПС України, ІПРЕЕД НАН України, СумДУ, ЛНТУ, НДІ СРП. Сімферополь : Фенікс. 2010. 582 с.

3. Ареф'єва О. В., Кузьменко Т. Б. Планування економічної безпеки підприємств. Київ: Вид-во Європ. ун-ту, 2005. 170 с.

4. Бабич Є. Ю. Забезпечення кібербезпеки в Україні : thesis. 2016. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/5102.

5. Батенко Л. П.Стратегія підприємства: підприємницький контекст. монографія / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана»; заг. ред.: Л. П. Батенко, Т. І. Решетняк. – Електрон. текстові дані. – Київ: КНЕУ, 2019. – 424 с.

6. Браіловський М. М., Дорошко В. О., Чирков Д. В., Шелест М. Е . Захист економічної інформації: Навч. посібник / За ред. проф. В. О. Хорошка: – К.: НАУ, 2012. – 78 с.

7. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / ред. В. Б. Толубко. Київ : ДУТ, 2015. 288 с. URL: https://dut.edu.ua/uploads/p_303_79299367.pdf

8. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення : монографія. Львів : Арал. 2018. 384 с.

9. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. Економіка і організація управління. 2014. № 1 (17). С. 54–60.

10. Вольовод А. Г. Проект Європейської конвенції про кіберзлочини // Захист інформації. Конфідент – 2021 – № 5

11. Воронкова В. Г. Основи підприємництва: теорія та практикум: навч. посіб. / В. Г. Воронкова. – К.:Ліра-К, 2014. – 455 с.

12. Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління, 2018. 94 с.

13. Діяльність суб'єктів господарювання : стат. зб. / за ред. М. С. Кузнєцової. Київ : Консультант, 2015. 455 с. 12. ko.com — URL: https://ko.com.ua/uyazvimosti_vpervye_za_mnogo_let_oboshli_fishing_v_rejtinge_ metodov_vzloma_136442

14. Живко М. О. Особливості нормативно-правового забезпечення інформації в комп'ютерних системах підрозділів МВС // Наук. Вісн. ЛДУВС: Сер. юрид. зб. наук. праць / Гол. ред. В. Л.Ортинський. – Л., 2017. – Вип. 1. – С. 288 – 293.

15. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Vol. 2, Num. 1. С. 27–32. URL : http:// nbuv.gov.ua/UJRN/hv_2016_2_1_7

16. Качковська Л., Малеончук Г., Зінюк Д. Інформаційний вплив в умовах гібридної війни. Міжнародні відносини, суспільні комунікації та регіональні студії. 2022. № 3 (14). С. 87–102. URL: https://doi.org/10.29038/2524-2679-2022- 03-87-102

17. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. 2016. № 3. С. 123-129. URL: http://dspace.nbuv.gov.ua/handle/123456789/24811.

18. Ковальчук Т. Т. Економічна безпека і політика: із досвіду професійного аналітика. – К.: Т-во "Знання", КОО, 2014. – 638 с.

19. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення: Монографія. – К.: Лібра, 2013. – 280с.

20. Колпаков В.М. Стратегический кадровый менеджмент [Текст] : учебное пособие / Г.А. Дмитренко. – 2-е изд., перераб. и доп. – К.:

МАУП, 2005. – 752 с.

21. Концепція інформаційної безпеки України. URL: http://mip.gov.ua/files/banners/Final%20Проект%20 концепції%20(Текст)%20-%2030.09.15.pdf.

22. Кравченко М.О., Бояринова К.О., Копішинська К.О. (2021). Управління ризиками. Навчальний наочний посібник. Київ : КПІ ім. Ігоря Сікорського, 2021. 432 с.

23. Кравчук П. Я. Сутність та передумови виникнення поняття корпоративної безпеки підприємства. Науковий вісник Волинського держ. Ун-ту ім. Лесі Українки. № 1. С.165–170.

24. Крихтіна Є. І. Соціальна політика та економічна безпека : монографія. Під заг. ред. д-ра екон. наук, проф. Крихтіна Є. І. Донецьк : Каштан. 2012. 336 с.

25. Лисенко Ю.Г. Модернізація фінансових систем: методологія та інструменти управління / авт. кол.; за ред. Ю. Г. Лисенко, Д. М. Жерліцина. – Полтава: ПУЕТ, 2017. – 359 с

26. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / Ліпкан В.А. Максименко Ю.Є., Желіховський В.М. – К. : КНТ, 2016. – 280 с.

27. Лозинський О.М. Економічна психологія : навч. посіб. / О. М. Лозинський; Нац. ун-т "Львів. політехніка", Громад. орг. "Львів. аналіт. дім" . - Вид. 2-е, допов. - Львів : Сполом, 2018. - 204 с.

28. Лужецький В. А., Кожухівський А. Д,, Войтович О. П. Основи інформаційної безпеки : навч. посіб. Вінниця : ВНТУ, 2016. 221 с.

29. Ляшенко О.М. Концептуалізація управління економічною безпекою підприємства: [монографія] / О. М. Ляшенко. — Луганськ: СНУ ім. В. Даля, 2015. — 400 с.

30. Маркіна І. А., Дячков Д. Н. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва. 2016. № 3(1). С. 80–88.

31. Мороз О. В., Карачина Н. П., Шиян А. А. Концепція економічної безпеки сучасного підприємства : монографія. Вінниця : ВНТУ. 2017. 241 с.

32. Мужанова Т. М. Засоби інформування й навчання персоналу у сфері інформаційної безпеки в умовах цифровізації. Зв'язок 2021. Т. 152 № 4, С. 14- 16. URL: DOI: 10.31673/2412-9070.2021.041416.

33. Музика Т. П. Теоретико-методичні аспекти ефективної системи економічної безпеки агропідприємницької діяльності. Науковий вісник Львівського державного університету внутрішніх справ. № 1. 2012. С. 151-162

34. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Видав. дім «Гельветика», 2017. 168 с.

35. Низенко Е. І., Каленяк Е. І. Забезпечення інформаційної безпеки підприємництва : навч. посіб. Київ : МАУП, 2006. 134 с.

36. Обліково-аналітичне забезпечення управління економічною безпекою підприємства : монографія / за заг. ред. А. М. Штангрета. Львів : Українська академія друкарства, 2017. 276 с.

37. Організаційно-правові основи захисту інформації з обмеженим доступом: Навч. посібник / А. Б.Стоцький, А. М. Гуз, А. І. Марущак та ін.; За заг. ред. В. С. Сідака – К.: Вид-во Європ. ун-ту, 2006. – 232 с.

38. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. URL: http://sophus. at.ua/publ/ 2014_04_17_18_kampodilsk/sekcija_4_2014_04_17_18/osoblivosti_organizaciji_informacijnoji_bezpeki_suchasnogo_pidpriemstva/54-1-0-931

39. Положення про технічний захист інформації в Україні, затверджене постановою Кабінету Міністрів України від 9 вересня 1994 р. № 632 // ЗП України. – 1994. – №12.

40. Попиріна О.О. Поняття про ідентифікацію. URL: https://sites.google.com/ site/identifikaciataautentifikacia/ponatta-pro-identifikaciu

41. Правові засади інформаційної безпеки України : монографія / П.

Д. Біленчук, Л. В. Борисова, І. М. Неклонський., В. О. Собина ; за ред. П. Д. Біленчука. Харків : 2018. 289 с.

42. Про Доктрину інформаційної безпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. URL : https://zakon.rada.gov.ua/laws/ show/47/2017

43. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX: станом на 1 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1089- 20#Text

44. Про захист інформації в автоматизованих системах: Закон України // Відомості Верховної Ради. 1994. – № 31. – 286 с.

45. Про основи національної безпеки України: Закон України від 19 червня 2003 р. // Офіц. Вісн. України. – 2003. – № 29. – Ст. 1433.

46. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від від 26.08.2021р. № 447.URL: https://zakon.rada.gov.ua/go/n0055525-21

47. Проценко П. П. Проблематика переходу до інформаційного суспільства // Політ. менеджмент. – 2014. – № 6 (9). – С. 129–137.

48. Смолєв Є. С. Дослідження шляхів та розроблення рекомендацій щодо підвищення можливостей виявлення загроз корпоративній інформаційній системі

49. Сороківська О. А., Гевко Л. В, Інформаційна безпека підприємства : нові загрози та перспективи. *Вісник Хмельницького нац. ун-ту.* 2010. № 2, т. 2. С. 32–35.

50. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. Державне будівництво. 2016. № 2. С. 19.

51. Технології захисту інформації. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

52. Ткачук Г. О., Щукіна О. В. Обліково-аналітичне забезпечення кадрової політики підприємства. Обліково-аналітичне забезпечення в умовах

управління фінансово-економічною безпекою підприємства: монографія; за заг. ред. д. е. н., проф. В.В. Немченко. Одеса: Фенікс, 2015. С. 31–45.

53. Указ Президента України “Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України” від 22 січня 2002 р. № 63/2002. // Відомості Верховної Ради України.

54. Флейчук М. І. Легалізація економіки та протидія корупції у системі економічної безпеки: теоретичні основи та стратегічні пріоритети в умовах глобалізації. Львів : Ахілл. 2008. 660 с.

55. Франчук В. І. Теоретичні засади корпоративної безпеки. Актуальні проблеми економіки. 2009. № 7. С.161–167.

56. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури / Ю. І. Хлапонін та ін. Кібербезпека: освіта, наука, техніка. 2022. Т. 3, № 15. С. 124–134. URL: https://doi.org/10.28925/2663- 4023.2022.15.124134

57. Чубаєвський, В. Методи управління корпоративною інформаційною безпекою.. Економіка та суспільство, № 43 (2022). URL: https://doi.org/10.32782/2524-0072/2022-43-49

58. Шостак Л.В. Зарубіжний досвід управління персоналом / Л.В. Шостак, Є. О. Болобан. // Приазовський економічний вісник. – 2018. – № 3 (08). – С. 94 - 99.

59. Шпикуляк О. Г. Інституції у розвитку та регулюванні аграрного ринку : монографія. К. : ННЦ ІАЕ. 2016. 396 с.

60. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

61. 10 ways businesses can prevent social engineering attacks - hitachi systems security. Systèmes de Sécurité Hitachi. URL: https://hitachi-systems-security.com/10- ways-businesses-can-prevent-social-engineering-attacks/.

62. 2015 Global Cybersecurity Status Repor. (2015, January). ISACA

International. Retrieved from https://www.isaca.org/cyber/ Documents/2015-Global-Cybersecurity-StatusReport-Data-Sheet_ mkt_Eng_0115.pdf

63. Abe, S. et al. (2016) ‘Security Threats of Internet-reachable Industrial Control System (ICS)’, in Society of Instrument and Control Engineers of Japan (SICE) Annual Conference 2016. Tsukuba: IEEE Xplore, pp. 750–755.

64. Ani, U. P. D., He, H. M. and Tiwari, A. (2016) ‘Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure’, in Nicholson, D. (ed.) Advances in Human Factors in Cyber Security: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA. Florida: Springer International Publishing, pp. 169–182

65. Cisco 2016. Annual Security Report. (2016). Cisco. Retrieved from http://signalpartners.fi /wpcontent/uploads/2016/01/Cisco-securityreport-2016.pdf

66. DaVeiga,A. and Eloff,J.H.P.(2010) “A framework and assessment in strument for Information Security Culture”, Computers &Security, Vol.29, No.2010.

67. David Kushner, "The Real Story of Stuxnet". IEEE Spectrum, March 2013.

68. IT best of breed. IT Best of Breed. URL: http://i.crn.com.

69. Hitt M. Strategic management: competitiveness & globalization. Concepts and cases / Michael Hitt. – Boston: Cengage Learning, 2017. – 743 p

70. Human factor security: evaluating the cybersecurity capacity of the industrial workforce Ani, Uchenna Daniel; He, Hongmei; Tiwari, Ashutosh Journal of Systems and Information Technology, Volume 21, Number 1, 2019, pp. 2-35(34).

71. Macrae I. High potential: how to spot, manage and develop talented people at work / I. Macrae, A. Furnham, M. Reed. – London: Bloomsbury, 2018. – 342 p.

72. https://mhp.com.ua/ Офіційний сайт ТОВ «МХП»

73. Parsons, K. et al. (2010) Human Factors and Information Security:

Individual, Culture and Security Environment, Science And Technology. Edinburgh South Australia. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf.

74. Parsons, K. et al. (2014) ‘Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)’, Computers and Security. Elsevier Ltd, 42, pp. 165–176.

75. Schneider B. Organizational Climate and Culture: Reflections on the History of the Constructs in JAP. California, 2017. 49 p. URL: https://psycnet.apa.org/doiLanding?doi=10.1037%2Fapl0000090

76. Sharkey L. The future-proof workplace: six strategies to accelerate talent development, reshape your culture, and succeed with purpose / L. Sharkey. – United States: John Wiley & Sons Inc, 2017. – 240 p.