DOI https://doi.org/10.36059/978-966-397-319-7-9

Розділ 9

НАПРЯМИ ПРОТИДІЇ ТА ЕФЕКТИВНОЇ БОРОТЬБИ З РЕЙДЕРСЬКИМИ ЗАХОПЛЕННЯМИ В СИСТЕМІ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

д. е. н., проф. Т. О. Меліхова, магістрант Є. В. Меліхов

9.1 ВИЯВЛЕННЯ ХАРАКТЕРНИХ ОЗНАК РЕЙДЕРСЬКОГО ЗАХОПЛЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Характерною рисою новітньої історії розвитку вітчизняного підприємництва є зростаюча кількість операцій, пов'язаних із злиттям, перетворенням та приєднанням суб'єктів господарювання, яке часто проявляється в досить агресивній формі, так званому недружньому поглинанні [3].

Одночасно з появою приватної власності з'явилися охочі заволодіти чужим майном незаконним шляхом. Вони почали розробку різних методів заволодіння власністю. Сам процес незаконного захоплення майна отримав назву «рейдерство».

Рейдерство (від англ. *Raider*, спочатку «учасник нальоту») – силове недружнє поглинання підприємства проти волі його власника, що має переважне становище на даному підприємстві, або керівника; процес, пов'язаний з рейдерством, називається «рейдерське захоплення» [6].

Вважаю, що у наш час недостатньо досліджені наступні питання: як рейдерське захоплення впливає на економічну політику держави та перерозподіл власності, які наслідки має рейдерство для України, чому люди не в захваті від рейдерства, які методи запобігання рейдерським захопленням.

Взагалі, тема рейдерства наразі привертає до себе багато уваги. Рейдерство стало практично буденним явищем для нашої країни. Рейдерством є поглинання підприємства проти волі його власника чи керівника [28].

«Рейдерство» по-українськи здебільшого полягає у набутті сумнівними шляхами тимчасового права розпоряджатися активами та якнайшвидшим продажем цих активів пов'язаним із рейдером особам, із наступними перепродажами вилучених активів між пов'язаними особами, маючи на меті завадити (унеможливити) їхньому поверненню законним власникам [29].

За словами відомого економіста Г. О. Грефа «очищення» слабких підприємств на законних підставах може бути корисним для економіки, однак в Україні все навпаки. Масштаб такого явища, як рейдерство, недооцінюється спостерігачами, а його руйнівність не тільки для економіки, але і для всього суспільства не викликає сумнівів. Багато юристів, журналістів, публіцистів і вчених досі сперечаються про те, що таке рейдерство, хоча всі розуміють, що з даним явищем потрібно боротися. Рейдерство часто носить кримінальний характер і активи відбираються у найбільш прибуткових підприємств [11].

DOI https://doi.org/10.36059/978-966-397-319-7-9

Серед розповсюджених типів рейдерських захоплень виділяють такі:

1) силове захоплення за допомогою спецслужб шляхом зміни керівництва та встановлення повного контролю на підприємстві;

2) боргове захоплення шляхом придбання кредиторської заборгованості;

3) захоплення за допомогою реєстратора (перешкоджання проведення зборів акціонерів, контроль рейдером реєстратора);

4) додаткова емісія;

5) придбання акцій;

6) контроль над менеджментом;

7) реприватизаційні захоплення;

8) юридичний терор;

9) інформаційний терор [11].

Типи рейдерських захоплень зображені на рис. 9.1 [21; 22; 24; 25].

Класичне рейдерське захоплення полягає в тому, що агресор намагається всіма правдами і не правдами отримати на скільки завгодно короткий термін формальний контроль над компанією-жертвою, що дозволяє проводити операції з її активами. У хід йдуть будь-які засоби: маніпулювання акціями і акціонерами,

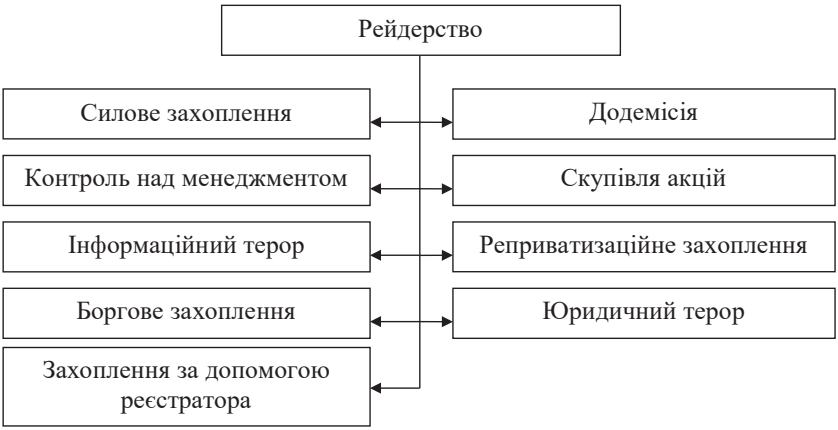


Рисунок 9.1 – Типи рейдерських захоплень

використання підроблених документів і, зрозуміло, залучення адміністративного ресурсу (судів, поліції та ін.) [11].

Хоча застосування слова «рейдерство» до корпоративного поглинання отримало розповсюдження нещодавно, захвати з'явились одночасно з акціями, які дали можливість поглинанню компанії незалежно від волі керівництва [28].

Захоплення власності може здійснюватися по-різному. Існує кілька видів рейдерських операцій, і далеко не завжди вони можуть приймати форми збройного конфлікту. Головне, що відрізняє такі операції – вони здійснюються проти волі власника, працівників підприємства або компанії, причому метою в більшості випадків є захоплення чужої власності або майна без належної оплати за нього.

До недавнього часу IT-компанії в поле зору рейдерів не потрапляли, так як найбільш привабливими вважаються ті підприємства, де вартість матеріальних активів (нерухомості, виробничого устаткування, земельних ділянок) істотно перевищує номінальну вартість самого бізнесу. За даними відомих аналітиків, рейдерства в сфері інформаційних технологій у цей час практично не існує. Вважається, що ринок IT-технологій нецікавий для рейдерів, тому що в ньому крутиться не так багато грошей, а, головне, тому що серед рейдерів немає фахівців, які могли б керувати IT-бізнесом. З огляду на той факт, що ринок IT зараз активно розвивається, тому цілком можливо, що рейдери, «відпрацювали» інші високоприбуткові сфери бізнесу та захочуть зайнятися і новими технологіями. Крім того, в IT може мати місце проблема не стільки рейдерства, скільки конкурентної боротьби, в ході якої будуть використовуватися елементи рейдерства. Теоретично можливе використання рейдерських схем, щоб видавити з ринку конкурента. У таких рейдерів у запасі безліч технологій. Це може бути як злом сайту, так і pr-технології: замовні статті або кілька судових позовів від покупців, які скаржилися на недоброякісну продукцію. У сфері IT рейдери можуть підприємство і не захоплювати, їм достатньо зробити його економічно невигідним. Отже, ми маємо справу ще з одним типом рейдерського

DOI https://doi.org/10.36059/978-966-397-319-7-9

захоплення, яке здійснюється шляхом викрадення або псування програмного продукту [11].

Дії IT-рейдерів не тільки розоряють окремі підприємства, але й істотно гальмують розвиток галузі загалом. Спостерігаючи за високими темпами розвитку українського IT-ринку, слід відзначити, що це зростання обумовлене внутрішнім попитом на IT-продукцію та IT-послуги. Для подальшого ж розвитку, вітчизняним компаніям необхідно виходити на міжнародний рівень, що потребує залучення серйозних інвестицій. Сьогодні ж більше половини всіх IT-компаній є інвестиційно непривабливими, оскільки будь-який інвестор, перш ніж приймати рішення, оцінює вигоди і ризики. На жаль, в ситуації, коли ризики не підлягають оцінці, коли об'єкт інвестицій знаходиться поза законодавчої бази, інвестор, як правило, вважає за краще не ризикувати, а це значить, що компанії недоотримають капітали, темпи їх зростання стають нижче, ніж могли б бути, і їх позиції на міжнародних ринках дістаються конкурентам [11].

Як не прикро визначати, але якщо компанія розробляє серйозний проєкт, то достатньо просто порушити строки його закінчення. Для цього може бути застосований простий мережевий вірус, який здатен оминути програмний захист та зіпсувати комп'ютерний код [32]. На жаль, програмісти не завжди роблять резервну архівацію даних під час написання програм, тому вони навряд чи встигнуть відновити програму навіть до попереднього рівня. Й мови нема про закінчення у відповідний термін. Саме це і потрібно рейдеру. Фахівці рейдерських груп прораховуючи «успіх» операції, здійснюють різні заходи [29]. По-перше, замовник (скоріш за все – людина, найнята рейдером) може звернутися до суду і виграти собі величезну компенсацію, вганяючи власника в борги, або запропонувати йому вигідний для себе компроміс. По-друге, заохочена особа може звернутися до правоохоронних органів. У разі написання заяви у відповідне відомство (наприклад, за порушення авторських прав працівниками даної компанії), правоохоронці мають право завітати на підприємство та вилучити обладнання (сервери, комп'ютери та інше), тим самим

просто паралізуючи подальшу роботу підприємства [31]. Компанія від таких дій нічого, крім збитків, отримати не може. Саме тому і почалося активне дослідження рейдерства. Щоб запобігти рейдерському захопленню потрібно розуміти, як воно відбувається, а щоб зрозуміти, як чинити спротив рейдеру, треба викрити його справжню мету [11].

Проведений аналіз дозволив дійти наступних висновків. В Україні сьогодні рейдерське захоплення ІТ-бізнесу є досить нищівним чинником, що впливає на безпеку як ІТ-підприємств, так і країни зокрема. Для мінімізації та уникнення рейдерських дій в ІТ-сфері пропонуємо наступне: комп'ютерам, які використовуються для написання програм на замовлення, не надавати можливість виходу до Інтернету; мати команду досвідчених юристів (бажано – з досвідом боротьби з рейдерством); прийняти законодавчі акти, які б не дозволяли рейдерам вдаватися до подібних заходів. Окрім того, з огляду на сучасні реалії, в яких опинилася наша держава це питання потребує постійного вивчення і напрацювання дієвих заходів з його уникнення [11].

Відношення до недружніх захватів поглинанням у більшості країн двояке, особливо в континентальній Західній Європі: там вважається, що рейдери зазвичай зацікавлені в короткострокових прибутках, що спонукає компанію до дієвості.

Вагомий внесок у дослідження теоретичних та практичних аспектів рейдерства внесли науковці, а саме: Д. В. Зеркалов, Ю. В. Терепіща, Ю. А. Хатнюк, Л. С. Яструбецька та багато інших [30]. Водночас питання комплексного впливу цих категорій на економічний розвиток залишається значною мірою невирішеним [5].

Судові позови окремих міноритарних акціонерів до підприємства – це вже перший привід придивитися і запідозрити недобре. В Україні вкрай мало міноритарних акціонерів, які відстоюють свої права в суді, і більш того – роблять це самотужки. Якщо в суд направлено позов міноритарія акціонера – це перший сигнал, який сповіщає про початок рейдерської операції, і в більшості випадків – основна частина цієї операції. Причому, зміст позову

DOI https://doi.org/10.36059/978-966-397-319-7-9

може бути фантастичною і навіть надзвичайною – рейдери рідко турбуються про достатні юридичні підстави для позову.

Варто звернути увагу і на те, що друкують ЗМІ. Якщо в масмедіа починають друкувати статті, які представляють підприємство в не дуже доброму світлі – це також може бути початком рейдерської операції. Подібних статей, як правило, з'являється дві-три. Кажуть вони про одне й те ж, але різними словами. Характерна риса: до вас ніхто не звертається за коментарями, в кращому випадку даються думки якийсь «третьої сторони». У нашу епоху «свободи слова» вимоги об'єктивності в загальному виконуються. Якщо журналіст через них переступив – значить, це і не журналіст, а ворожий «писака». Можуть бути і «замовні сюжети» по телебаченню.

Часті перевірки підприємства з боку всіляких органів теж повинні насторожити зацікавлені сторони. Чим масовіше такі перевірки і чим більше сміховинні приводи до них – тим більша ймовірність наявності спланованої рейдерської операції.

Нарешті, поява мітингувальників під стінами підприємства. Молодих людей і людей середнього віку змусити вийти на мітинг може тільки один фактор – гроші. Вирішувати реальні проблеми в разі їх виникнення (затоплення будинку, відсутність опалення тощо) громадяни вважають, що краще послати «ініціативну групу» до відповідних інстанцій. Мітинг ж біля стін заводу – захід в ста відсотках випадків оплачене. А хто стоїть за мітингом і які в нього цілі – розмова окрема.

Велика кількість людей, які не є дуже освіченими в галузі захисту даних, звикла чути слово «рейдер» та вважають, що єдиною його метою є злиття або поглинання підприємства для того, щоб захопити гроші фірми-жертви [23]. Але рейдери, в першу чергу, мають за мету заволодіння саме фінансовими активами підприємств. Не всі знають, що ці поняття зовсім не одне й теж саме, скоріш – навпаки.

Гроші – це спеціальний товар, який є вираженням цінності інших товарів та послуг, є носієм купівельної спроможності та приймається у якості оплати. Фінанси – це економічні

відносини, які пов'язані з формуванням, розподілом і використанням грошових коштів [8].

Тобто, фінанси – це управління грошима. Саме це управління і бажає захопити рейдер.

Але здійснити злиття не так просто, як здається на перший погляд. Воно ніколи не відбудеться без економічного прогнозу, бо інакше це може бути не рентабельно і завдати лише збитків. Вдаватися до цієї процедури стануть тільки після того, як буде надано реальну оцінку всім можливим позитивним та негативним ефектам від злиття [27]. Саме тому, якщо злиття все ж таки відбувається – воно піде лише на користь всім зацікавленим сторонам [7].

Самим простим способом запобігти йому – це використання безготівкових розрахунків у будь-якій сфері діяльності підприємства: розрахунки з постачальниками, з працівниками, з податковою.

Завдяки цьому, підприємцям значно легше контролювати витрати, адже в особистому кабінеті буде видно, хто і куди витратив певну суму грошей [1]. Отже, рейдер не може здійснити жодного платежу й залишитися непомітним, адже така транзакція здається підозрілою фінансовому відділу і він її просто не пропустить.

Для того, щоб протистояти рейдерству, потрібні спеціалісти високого рівня. В першу чергу, не можна забувати про захист технічних пристроїв фірм, адже через них можна отримати доступ до слабких місць компанії та використати їх при здійсненні рейдерського захоплення. Зараз, на нескінченних просторах Інтернету, можна знайти велику кількість інформації про викрадення даних зловмисниками з приладів користувачів. Люди, підприємства і навіть держава зазнають величезних збитків. Все це відбувається через те, що багато розробників приділяють велику увагу інтерфейсу програми, зручності користування тощо. Але найбільша проблема криється у безпеці. Нікому не потрібна надзвичайно красива та зручна програма, якщо ваші дані можуть з неї викрасти. Це теж саме, що залишити дірку в паркані, сподіваючись на те, що її ніхто не знайде [10]. До того ж, часто

DOI https://doi.org/10.36059/978-966-397-319-7-9

підприємці й самі не приділяють потрібної уваги безпеці даних. Вони використовують первісні засоби захисту та вважають себе у безпеці, насправді залишаючи безліч можливостей для зловмисника. Саме через такі «прогалини в обороні» вони і втрачають цінну інформацію, а разом з нею і власні кошти. Наприклад:

- можливість вільної зміни програмного коду;
- відсутність відстеження внесених змін в код програмного застосування;
- відсутність відповідності надаваної інформації функціональними обов'язками співробітника або такий фільтрації на підприємстві взагалі;
- відсутність резервних копій документів підприємства в різних місцях;
- часте внесення правок і проведення рефакторингу програм різними технічними фахівцями.

Саме для цих цілей на підприємстві й існує Служба інформаційної безпеки. До її обов'язків входить:

1) розробка способів виявлення загроз, оцінки фактичного рівня інформаційної безпеки даного підприємства і систем, які її забезпечують;

2) організація і здійснення конкретних видів діяльності із захисту інформації;

3) експлуатація різних існуючих технічних засобів захисту інформації;

4) проведення аудиту і контролю стану інформаційної безпеки підприємства [4].

У більшості випадків служба інформаційної безпеки сформована із колишніх працівників органів внутрішніх справ по боротьби з кіберзлочинністю, які достатньою мірою володіють потрібними знаннями та вміннями щодо здійснення внутрішнього контролю. Програмісти володіють цим питанням, але не володіють знаннями з методики проведення перевірки. Цією методикою достатньою мірою володіють державні та сертифіковані аудитори. Якщо робота державної аудиторської служби пов'язана з пошуком недоліків у веденні обліку та складанні звітності з метою

накладання фінансових санкцій за виявлені порушення, то сертифіковані аудитори залучаються власниками підприємств на комерційній основі для перевірки окремих об'єктів обліку та звітності з метою виявлення та подальшого самостійного усунення помилок, щоб уникнути майбутніх штрафних санкцій.

Підприємствами приділяється значна увага інформаційній безпеці, коли існує вірогідність рейдерського захоплення підприємства, витоку або передачі інформації третій стороні, втрат від неконтрольованого виносу матеріалів, товарів, готової продукції. У разі виявлення шахрайських дій та зловживання службовим становищем працівниками підприємства, перевіряючими органами передбачені фінансові санкції за порушення законодавства, які можуть бути попереджені службою інформаційної безпеки підприємства. При створенні відділу керуються співвідношенням можливих отриманих доходів та зниженням втрат підприємства порівняно із загальною сумою витрат на утримання служби, які включають матеріальні витрати (на канцелярію), витрати на оплату праці, нарахування єдиного соціального внеску на фонд оплати праці, амортизацію обладнання, інші операційні витрати (на відрядження). У даному випадку витрати легше оцінити ніж доходи та вигоди, які надає служба інформаційної безпеки підприємства.

Служба інформаційної безпеки великого підприємства може включати в себе відділи (рис. 9.2): комп'ютерного та серверного обладнання, програмного забезпечення, охорони, персоналу (розробники, програмісти), боротьби з кіберзлочинністю.

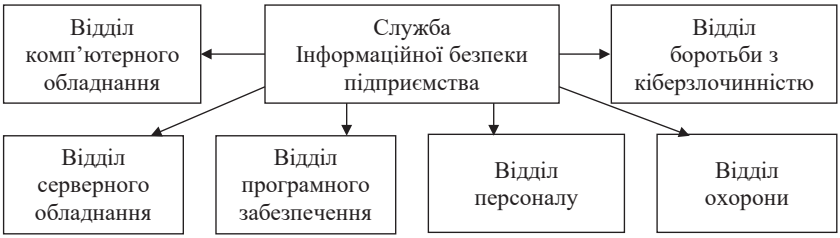


Рисунок 9.2 – Удосконалена структура служби інформаційної безпеки великого підприємства

DOI https://doi.org/10.36059/978-966-397-319-7-9

У підприємства завжди є вибір – створювати службу на підприємстві або користуватись послугами фірм з розробки програмного забезпечення. Оптимізація структури та штату відділів підприємства є напрямком економії витрат підприємства.

Служба інформаційної безпеки середнього підприємства може включати в себе один відділ з підрозділами, у якому працюють: програміст, розробник, охоронці, технік, системний адміністратор (рис. 9.3).

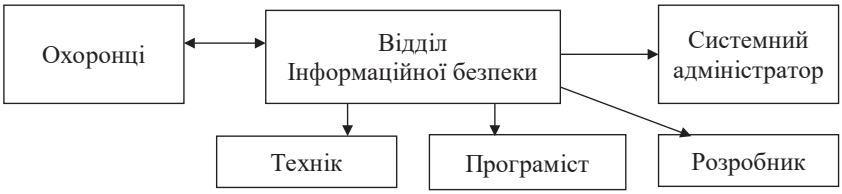


Рисунок 9.3 – Удосконалена структура служби інформаційної безпеки середнього підприємства

Відділ інформаційної безпеки включає в себе: працівників служби внутрішнього аудиту, які здійснюють внутрішній контроль, проводять інвентаризацію, перевіряють роботу персоналу підприємства та дотримання ним посадових інструкцій, проводять аналіз господарської діяльності, фінансових аналітиків, які нейтралізують негативні дії від загроз та рейдерських атак, попереджують про можливі збої обладнання та заміну програмного забезпечення, запобігають кіберзлочинам та правопорушенням.

Оптимальна штатна чисельність працівників служби інформаційної безпеки підприємства повинна бути сформована з врахуванням обсягу виробництва та специфіки його діяльності, існуючих зовнішніх та внутрішніх загроз, мати змогу виявляти недоброчесних контрагентів та конкурентів, а також забезпечувати протидію спробам захоплення інформації підприємства. Завдання інформаційної служби безпеки полягають у забезпеченні цілісності майнової та інтелектуальної власності підприємства, захист фінансових, інформаційних та правових його інтересів, контроль за комп'ютерним та серверним обладнанням, програмним забезпеченням та його кадрами.

Але ні для кого не є таємницею, що останнім часом людство прогресує стрімкими темпами. За останні десять років кожна галузь досягла більшого розвитку, ніж за попередні п'ятдесят. В сьогоденні для подальшого зростання необхідна не тільки сучасна техніка, а й висококваліфіковані професіонали, які здатні пристосовуватися до швидкого прогресу.

Це означає, що неможливо навчити людину чомусь один раз і на все життя. Для повноцінного існування їй необхідно постійно вдосконалюватися [14]. Тільки така людина може ефективно протистояти намірам недружнього поглинання, а можливо й не одна. Інтенсивний розвиток великих проєктів вимагає створення технологій колективної розробки продукту і формування творчого колективу [13]. До того ж, навіть якщо людина не знає якогось сучасного методу боротьби з хакерами – їй ніхто не заважає цьому навчитися.

Згідно з висловлюванням Елвіна Тоффлера, американського соціолога та автора концепції «інформаційної цивілізації», безграмотними людьми XXI ст. є не ті, хто не вміють читати і писати, а ті, хто не можуть вчитися, забувати те, чому навчилися, й переучуватися. Зараз навіть непотрібно витрачати купу часу на дорогу до навчального закладу. Можна вчитися майже будь де. Зараз суспільству значно легше саморозвиватися, адже існує велика кількість інтернет-курсів, наприклад, можна слухати аудіокурс з іноземної мови у вільний час. Окрім того, з'являється багато симуляторів, які потрібні для більш детального розуміння механізму роботи якоїсь системи та оволодіння практичними навичками роботи з нею [12].

Але використання інтернету не обмежується лише сферою навчання. Більшість людей, працюючих на підприємствах, починають свій ранок з робочої наради, так званої «п'ятихвилинки». На них керівництвом освітлюється план роботи, ставляться завдання та слухаються звіти про виконану роботу. Але якщо це підприємство має власні філії в різних частинах міста або взагалі – регіону, то фізично збирати кожного ранку на нараду їх керівників і невигідно (адже вони витрачають гроші фірми

DOI https://doi.org/10.36059/978-966-397-319-7-9

на дорогу в обидві сторони), і незручно (оскільки вони витрачають на це час та енергію, які можна було б направити на вирішення робочих питань). Повністю відмовитись від робочих нарад вкрай важко, адже від чіткості поставленої задачі залежить якість її виконання. Але зовсім відмовлятися від них непотрібно тому, що можна просто змінити їх формат. У такому випадку на допомогу можуть прийти дистанційні наради за допомогою мережі Інтернет [2].

Під час створення схожих за призначенням програмних застосунків абсолютно різні програмісти використовують схожі (або, навіть, однакові) технології. Через це в них виходять майже ідентичні програми [16]. Зараз існує не один десяток інтернет-платформ, за допомогою яких можна проводити дистанційні наради. І всі вони мають майже однаковий інтерфейс. Для цього не потрібно ані надто швидке інтернет-з'єднання, ані просунений комп'ютер. За допомогою таких платформ всі можуть бачити обличчя один-одного, завантажену презентацію або віртуальну дошку. Для такої наради буде достатньо використовувати навіть власний смартфон. Але якщо при проведенні звичайної зустрічі ви можете бути впевнені в том, що все те, що ви кажете, почують лише ваші підлеглі, бо ваш голос передається за допомогою коливань повітря, то при використанні Інтернету дані передаються по мережі [2]. Через це хакерам не складе великих труднощів отримати доступ до інформації підприємства [15]. Для запобігання цьому потрібно обирати платформи, де використовуються методи шифрування інформації [2].

Шифруванні інформації – це процес, завдяки якому інформація, що передається мережею становиться незрозуміла для людини або програми, в якої немає ключа. Для того, щоб інформація отримала свій початковий вигляд, потрібно провести процедуру дешифрації за допомогою ключа. Для надійності шифрування може проводитися декілька разів [2].

9.2 ВИКОРИСТАННЯ БЛОКЧЕЙНУ ДЛЯ ЗНИЖЕННЯ ВІРОГІДНОСТІ РЕЙДЕРСЬКОГО ЗАХОПЛЕННЯ З МЕТОЮ ДИДЖИТАЛІЗАЦІЇ УКРАЇНСЬКИХ ПІДПРИЄМСТВ

В епоху диджиталізації ні для кого не є секретом, що вся інформація про різноманітні угоди (разом з цим і персональні дані) переходять з великих картотек на цифрові носії. Не має значення, що саме це за дані: чи то операції з цінними паперами, чи продаж квартири, чи переказ коштів. У диджіталізації є незаперечний плюс. Якщо подивитися на ситуацію з боку отримання необхідної інформації, то електронна версія, безперечно, зручніша, ніж архівні документи. Адже для відповіді на вихідний запит достатньо лише вибрати необхідний тип інформації, що запитується, і ввести наявні дані. Вже через кілька секунд дані будуть перед вами, якщо вони є в сховищі. Але залишається відкритим питання їхньої безпеки. Він і раніше був із найпростіших, оскільки всі ці архіви потрібно було захищати від проникнення сторонніх осіб. Але в тому випадку, якщо дані передаються по мережі, можливість попадання їх у сторонні руки стає значно ймовірнішою. І вже не важко змінити потік інформації і зробити так, що новим власником активу стане людина, яка не брала участі в угоді. На початковому етапі диджиталізації обходилися шифруванням запитів і відповідей, це рятувало у тих випадках, коли зловмисники намагалися перехопити або просто «прослухати» відповідь, але абсолютно не рятувало у разі спроби зміни інформації, що передається. Незабаром, для цього було розроблено спеціальну технологію, названу «Блокчейн» [9].

Серед його ключових аспектів можна зазначити наступне:

1. Зберігання інформації. У світі немає абсолютно захищеного носія даних. Будь-яку інформацію можна отримати різними способами: від крадіжки жорсткого диска до злому хмарного сховища. В епоху, коли багато сфер промисловості набули всесвітнього масштабу, надзвичайно важливо уникати складних операцій з переміщенням даних, щоб запобігти витоку важливої інформації

DOI https://doi.org/10.36059/978-966-397-319-7-9

та зменшити ймовірність помилок. Використання блокчейн технології здатне вирішити ці проблеми Викрасти інформацію, що знаходиться фізично на різних пристроях у різних частинах світу, практично неможливо. Злом і викрадення даної інформації теж є вкрай скрутним у зв'язку з тим, що недостатньо володіти інформацією про єдиний ланцюжок.

2. Авторське право. Останнім часом виникло безліч популярних сервісів на підтвердження авторського права, серед яких: Proof of Existence, Emernotar, Депонент. Технологія блокчейн дозволяє створювати електронні копії робіт, ідентифікувати унікальність знаків та символів, отримувати сертифікати автентичності у цифровому вигляді.

3. Ідентифікація особистості. Підтвердження особистості великих інформаційних гігантів, таких як Microsoft, Apple, SpaceX вже давно відбувається за допомогою відбитка пальця, сканування обличчя або сітківки ока. Зрозуміло, що компанія з багатомільярдним прибутком не ризикуватиме своїми коштами та заощаджуватиме на безпеці. Зламати їх сервер та змінити параметри відбитка ока, щоб отримати права керівника підприємства та розпоряджатися фінансами – неможливо через відсутність його. Завдяки блокчейну інформація просто не зберігається в одному місці.

4. Блокчейн інтелектуальному інтернеті речей. Багато платформ активно впроваджуються та використовуються для отримання даних користувача, зберігання інформації, пов'язаної зі споживчою поведінкою. Прикладом такої блокчейн-технології є Chronicled. Ще далі у напрямку ідентифікації речей у процесі товарообігу пішла платформа Ethereum. Її команда розробила свою систему, основним завданням якої є чіпування предметів, що у продажу. Це можуть бути як дешеві товари супермаркету, так і ексклюзивні моделі для колекціонування. Така технологія дозволяє покупцю чи продавцю в режимі реального часу відстежити шлях пересування продукції, відстань від пункту призначення, віддаленість від власника [9].

Отже, викликані блокчейними інноваціями в різних сферах допоможуть вивести їх розвиток на новий рівень, підвищити

прозорість процесів, знизити ризики та збільшити ефективність функціонування процесів управління. Виявлені переваги технології блокчейн дозволять використовувати її для побудови найсучасніших безпечних додатків [9].

Зараз, на нескінченних просторах Інтернету, можна знайти велику кількість інформації про викрадення даних зловмисниками з приладів користувачів. Люди, підприємства і навіть держава зазнають величезних збитків. Все це відбувається через те, що багато розробників приділяють велику увагу інтерфейсу програми, зручності користування тощо. Але найбільша проблема криється в безпеці. Нікому не потрібна надзвичайно красива та зручна програма, якщо ваші дані можуть з неї викрасти. Це теж саме, що залишити дірку в паркані, сподіваючись на те, що її ніхто не знайде. Для того, щоб дані користувача залишилися у безпеці та жодна людина не мала до них несанкціонованого доступу існує захищене програмування. Його використання дозволяє уникнути важких, а іноді й фатальних, наслідків роботи програми за рахунок застосування спеціальних прийомів раннього виявлення і нейтралізації помилок. Програмуванням з захистом від помилок дозволяє розробникам програмних за стосунків не чекати зловмисника, який знайде прогалини в безпеці та скористається ними, а ліквідувати їх на етапі розробки програмного забезпечення самостійно [10].

Вже багато років спеціалісти зі всього світу намагаються з'ясувати, як саме можна ліквідувати найнебезпечніші прогалини у безпеці програм. Але для усунення цих недоліків потрібно спочатку їх визначити. Найбільш поширеними прогалинами в безпеці програм, на поточний час, визнані:

– переповнення буферу. Відбувається або коли в програму намагаються ввести більше інформації, ніж вона може обробити, або в разі введення некоректного символу. Запобігти можна, якщо зробити перевірку вхідного рядка на кількість символів та на їх коректність;

– некоректна автентифікація. Часто користувачі обирають дуже прості паролі навіть не здогадуючись, що у їх акаунт можна

DOI https://doi.org/10.36059/978-966-397-319-7-9

увійти простим перебором паролів. Логіка проста: «Це ж скільки часу потрібно, щоб підібрати мій пароль». Зловмисники ніколи не роблять цього вручну. Вони використовують спеціальні програми, які просто перебирають можливі варіанти з великою швидкістю. Запобігти можна зробивши програмні обмеження на формат паролю: довжина, спеціальні символи, великі літери;

– перехоплення інформації. Якщо використовується слабкий механізм шифрування зловмисник може отримати доступ до інформації перехопивши її. Запобігти цьому можливо завдяки використовуванню складних алгоритмів шифрування;

– обробка помилок та виключень. Під час виконання програми може виникнути помилка, дії для якої не передбачені. У такому разі зловмисник може перехопити керування програмою і далі вона буде працювати за його власним сценарієм. Запобігти цьому можна зупиненням виконання програми у разі виникнення помилки, якщо не прописано інших дій.

Саме через вищенаведені причини частіш за все і виникають витоки інформації до сторонніх осіб. Якщо ж розробляти програму згідно з потребами захищеного програмування, то ризики зламу будуть значно мінімізовані. Зробити продукт повністю захищеним на сто відсотків неможливо, адже який захист не розробила би одна людина інша завжди зможе її зламати. А відповідно – і отримати повний доступ до персонального пристрою користувача. Саме тому захищене програмування потрібно використовувати для будь-якого застосунку. Не має значення, що саме знаходиться у розробці: онлайн-банкінг, поштова скринька або програма для відображення громадського транспорту на карті міста. Адже зловмисник може використати будь-яку вразливість. Навіть якщо не використовуються жодні користувацькі дані, при наявності прогалині в безпеці програми можна отримати доступ до всього пристрою. А далі непроханий гість може робити все, що йому заманеться. Саме тому в застосунку потрібно шукати всі можливі недоліки та способи проникнення до неї. Бо якщо програма отримає славу «відкритих воріт для зловмисника» – це буде не найкраща реклама для розробника [10].

Обрана нами стратегія, програмування із захистом від помилок, або явне додавання обробки помилок, безпосередньо залежить від області застосування розроблюваного програмного продукту. Її своєчасне використання по перше, істотно зменшить ймовірність отримання невірних результатів, по друге, дозволить при написанні будь-яких програмних застосунків приділяти посилену увагу саме безпеці. Адже втрата контролю над однією (хай і не дуже важливою) конкретною програмою може означати втрату контролю над всім пристроєм разом з особистою інформацією, яка на ньому знаходиться [10].

У наше сьогодення гостро стала проблема створення сучасних інформаційних систем для різних галузей суспільства. І це не дивно, адже впровадження електронно-цифрових рішень на підприємствах дозволяє значно підвищити ефективність праці. Цей процес має назву «диджиталізація», під якою розуміють перенесення інформації з фізичних об'єктів (фотографії, документи, плівкові відеокасети тощо) на цифрові носії. Більшість науковців розуміє під цим процесом не просто створення більш захищених та надійних копій, а і здійснення розгортання місця зберігання (частіше всього – хмарного сховища або сервера), функцій аналізу даних, їхньої систематизації та внесення до системи. Здійснювати диджиталізацію та отримувати переваги від неї можна не тільки виробничим службам, але і економічному сектору. Перевагами є: мінімізація можливості здійснення механічних або випадкових помилок; зменшення ймовірності створення та ведення чорної бухгалтерії; можливість миттєвого отримання необхідної інформації; послаблення гніту паперової бюрократії. До того ж, держава постійно сприяє прискоренню диджиталізації на законодавчому рівні [17].

Вже не один рік народні господарства України застосовують у поєднанні 2 відомих програмних продуктів: один відповідає за бухгалтерські процеси (1С: Підприємство або його клон – BAS. Бухгалтерія для України), а інший – для ведення діловодства та подачі фінансової звітності (M. E. Doc). Проте, у зв'язку із забороною першого, виникла необхідність у пошуку заміни. Тож,

DOI https://doi.org/10.36059/978-966-397-319-7-9

зараз для кожного з підприємств постало питання: шукати дозволену альтернативу національного виробництва, розробити новий модуль для бухгалтерського обліку або створити унікальний програмний застосунок, у якому будуть поєднуватись всі функції, які необхідні суб'єктам народного господарства. Впровадження додатку дозволить вирішити одразу низку питань:

1. Частина документів підприємства ведеться не у спеціальних програмних застосунках, а у звичайних Word та Excel. Вони суворо типізовані і відрізняються один від одного лише обсягом та даними. Але будь-який імпорт до інформаційної системи, рано чи пізно, призведе до помилок або невідповідностей. Через це правильніше всю інформацію зберігати всередині застосунку, а у разі потреби – експортувати її у потрібному форматі.

2. Деякі підприємства використовують «галузеві програми». Це інформаційні системи, які полегшують працю штатних співробітників певного направлення, проте створюють додаткове фінансове навантаження на фірму. Зручніше було б використовувати певний режим у тому ж застосунку, яким здійснюється загальне керування підприємством. При застосуванні такий модуль можна налаштувати на друк або формування переліку в бажаному стилі. Це дозволить економити час, за рахунок створення шаблону розташування інформації у документі на власний розсуд ще на етапі його генерації.

3. Зникає необхідність оплачувати не лише вартість «галузевих програм», а й додаткову ліцензію за застосунок для діловодства та подачі фінансової звітності. Сукупність усіх цих програмних застосунків створює і справді відчутне фінансове навантаження на підприємство [17].

Частіше всього підприємства обирають саме розробку інформаційної системи у настільному форматі (desktop-застосунок), адже він містить велику кількість переваг.

1. Першим та, мабуть, найважливішим питанням стає забезпечення того, щоб дані не потрапили у треті руки (конкурентів або зловмисників). Найбільш використовуваними методами захисту є: блокування портів USB, щоб неможливо було скопіювати

інформацію на флешку; встановлення серйозних антивірусних та анти-шпигунських програм, щоб унеможливити викрадання дані через Інтернет; у випадку зберігання всередині внутрішній мережі підприємства інформації, яка є надважливою або вкрай секретною – взагалі забороняють підключати комп'ютер до «світової мережі».

2. Десктопна версія застосунку має більш високу автономність, забезпечує доступ до самого сайту та інформації, збереженої на віддалених серверах, без додаткових зусиль.

3. Швидкість роботи десктопного застосунку буде значно швидше, ніж у його вебверсії. Так, безперечно на дуже слабких та старих персональних комп'ютерах можуть виникати певні затримки у роботі. Проте основні простої системи, скоріш за все, будуть пов'язані із швидкістю отримання інформації з серверу, ніж із завантаженням сторінки або модулю, що ставить вебверсії подекуди навіть у більш скрутне становище [17].

Отже, спираючись на вищезазначені пункти, можна дійти до висновків, що створення єдиної інформаційної системи для підприємства у вигляді desktop-застосунку – це найбільш ефективне рішення у сучасних умовах. Воно надає можливість більш раціонально використовувати фінансові ресурси у довгостроковій перспективі [17].

Після Четвертої цифрової революції, яка охопила світ у кінці XX ст., всі остаточно зрозуміли, що у майбутньому комп'ютерні рішення повністю замінять існуючи методи роботи підприємств. Там, де раніше був потрібен труд декількох десятків людей, тепер цілком впорається одна сучасна інформаційна система. До того ж, працювати можна буде не лише з новими даними, а й із вже існуючими. Але для того, щоб можна було взагалі працювати із подібною інформацією у програмі, її необхідно цифровізувати. Згодом цей процес отримав назву диджиталізація [18].

Диджиталізація – це сучасний та інноваційний підхід, який містить у собі поєднання фізичних та цифрових можливостей у різних галузях життя людей, народного господарства та держави. Він може надати можливості для значного підвищення

DOI https://doi.org/10.36059/978-966-397-319-7-9

ефективності та надійності у роботі підприємств. Наприклад, дуже велику роль на будь-якій фірмі займає саме бухгалтерія. Отже, це один з перших підрозділів, який повинна буде оптимізувати диджиталізація. До того ж, велика кількість економістів погоджуються з тим, що майбутнє бухгалтерії саме за цифровими носіями. Наприклад, автори статті зазначають, що впровадження інформаційної системи для ведення обліку, дозволяє впорядкувати його, зменшити кількість помилок, підвищити ефективність відділу і його економічність та збільшити обсяг інформації, яку можна отримати у короткий термін» [18].

Але здійснення бухгалтерських проведень – це не єдина функція бухгалтерського відділу. Окрім цього вони займаються веденням діловодства, а це, як зазначили у своєму дослідженні Siemens Business Services, викликає певну кількість витрат та уповільнює діяльність підприємства. Наприклад:

- майже з кожного документу знімають копію до 20 разів;
- 30 % відсотків часу займає їх пошук та погодження;
- 6 % губляться та більше не знаходяться [18].

Диджиталізація цих функцій дозволить підвищити продуктивність підрозділу на 20 %, а вартість збереження електронних файлів замість паперових нижче на 80 %. Але ще більшої ефективності можна досягти завдяки зміни ідеї використання декількох програмних продуктів, які відповідають за свою функцію, на створення та використання єдиної інформаційної системи керування підприємством.

Взагалі, ідея об'єднання кількох програмних продуктів, які використовуються на фірмі, задля підвищення ефективності і створення єдиного інформаційного простору, існує доволі довгий час. Впровадження такої системи надає велику кількість переваг, а саме:

- уникнення можливих помилок при перенесенні даних з однієї програми до іншої;
- зменшення фінансового навантаження на підприємство, адже за кожну ліцензію на програмний застосунок необхідно платити гроші;

- можливість легкого впровадження додаткового функціоналу, який пов'язаний з діяльністю фірми [18].

Але до таких об'єднаних інформаційних систем існують певні вимоги, які необхідні виконуватися для дійсного підвищення ефективності підприємства. Отже, програмний продукт повинен:

- здійснювати збір, систематизацію та обробку інформації;
- проводити пошук, аналіз і оцінку джерел інформації для проведення економічних розрахунків;
- використовувати сучасні прийоми і способи для вирішення економічних завдань;
- використовувати сучасні наукові методологічні та методичні розробки економістів при проведенні аналітичних заходів;
- розробляти напрямки з мобілізації невикористаних резервів, впровадження інноваційних технологій [18].

Отже, диджиталізація здатна значно підвищити не лише ефективність окремих відділів, а й усього підприємства загалом. Проте, цільове використання різних програмних застосунків для підрозділів фірми не дадуть змогу повноцінно оцінити всі переваги від сучасних цифрових рішень. Саме через це значно ефективнішою буде використання єдиної інформаційної системи для керування підприємством [18].

З першого погляду може бути незрозуміло, навіщо все так ускладнювати, якщо мова йде про просту ранкову нараду. Так, можна використовувати майже будь-яку програму або онлайн-ресурс, якщо надана інформація не містить нічого таємного. Наприклад, проводити шкільні заняття онлайн можна за допомогою будь-якої програми, адже розголошення подібної інформації не призведе до негативних наслідків. Більш того, основна частина таких онлайн-уроків буде пізніше викладена вчителем до Інтернету з вільним доступом, щоб діти могли повернутися до матеріалу в тому випадку, якщо відволіклись або щось не зрозуміли. До того ж, жоден хакер не буде прослуховувати шкільний урок, адже його мета отримати вигоду від інформації, яку він викрав, а тут ніякої вигоди немає. Звичайно, якщо мова йде про якийсь тренінг від всесвітньовідомого «гуру» в своїй області,

за прослухання якого потрібно, наприклад, викласти одну тисячу гривень, збереження даних має важливе значення. В такому випадку цей тренінг можна прослухати, записати та викласти у Інтернет, де всі охочі можуть з ним ознайомитись, заплативши значно дешевше, але вже у кишеню хакера. Майже така сама ситуація може бути і на будь-якому підприємстві. На нараді може обговорюватися таємна стратегія, прихований від інших фірм власний інгредієнт та інше. Одним словом – все, що можна назвати «комерційною таємницею». У разі потрапляння подібної інформації до рук конкурентів вони можуть використати її для вдосконалення позиції власного підприємства на ринку. Але такі дії, звичайно, переслідуються законом. У тому випадку, якщо підприємство подасть заяву в правоохоронні органи, буде проведено розслідування і з високим ступенем ймовірності вдасться встановити факт викрадення інформації. Після цього буде судове засідання, за результатами якого вам може бути призначена компенсація за нанесені збитки. Для визначення розміру збитків будуть залучені співробітники науково-дослідного експертно-криміналістичного центру МВС України, які і будуть встановлювати втрати від подібного втручання в роботу підприємства. Але набагато простіше буде не доводити справу до судового розгляду, що забере багато сил і часу, а відразу впроваджувати таку технологію дистанційних нарад, в надійності якої ви будете впевнені [2].

Саме завдяки вищенаведеним факторам ризик рейдерського захоплення підприємства значно знижується.

Отже, виявлено, що досліджені фактори дозволяють нівелювати ризики рейдерського захоплення підприємства. Їх використання значно ускладнює підготовку та збирання інформації зловмисниками, яку можна використати для подальшого нападу.

9.3 ПРОПОЗИЦІЇ ЩОДО ЕФЕКТИВНОЇ БОРОТЬБИ З РЕЙДЕРСЬКИМ ЗАХОПЛЕННЯМ ЗА ДОПОМОГОЮ СУЧАСНИХ УПРАВЛІНСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Вчасно помітити підготовку рейдерської операції – вже пів справи і запорука перемоги. Пора переходити до другого кроку – широкий розголос. На цьому етапі знадобиться два підготовчих заходи. По-перше – найняти хороших юристів, по-друге – найняти хороших піарників. Важливий момент: і ті, й інші повинні мати досвід роботи з рейдерами.

Юристів необхідно налаштувати на протидію позовами, піарників – на створення інформаційного буму навколо рейдерської атаки. Рейдер – хоч і замаскований, але злодій. Він боїться розголосу своїх дій, вважає за краще діяти або зовсім нишком, або за «димовою завісою» судових рішень, пропаганди в пресі або вуличних мітингів.

Нарешті, третій крок – це звернення до влади. Якщо ширше – пошук союзників. Влада зацікавлена в збереженні власності. Капіталістичні держави – до яких ми себе зараховуємо – взагалі стоять на цьому. Рейдери в структуру такої держави не вписуються, навіть якщо ці рейдери сидять в уряді. І за законом, і, як то кажуть, «за поняттями», держава повинна вжити заходів до захисту підприємців. Але цілком покладатися на державу все ж не можна: вона неповоротка, законодавство у нас суперечливе.

Варто також розширити коло союзників:

- перше коло – жертви аналогічних захоплень;
- другий – різні асоціації та альянси, банки та інвестиційні фонди, аналітики і аналітичні центри.

Отже, врятуватися від рейдерського захоплення можна завдяки співпраці з досвідченими юристами та піарниками, які дадуть підприємцю можливість втримати контроль над власністю. Завдяки вказаним діям власник має змогу зберегти власне підприємство та захистити його від підготовлюваного нападу.

DOI https://doi.org/10.36059/978-966-397-319-7-9

Для ефективного відбивання рейдерських атак на підприємства необхідно вносити відповідні зміни на державному рівні. Подібними заходами можуть бути:

1) створення і впровадження відповідної бази даних, в якій будуть вказані подібні прецеденти по іншим підприємствам;

2) створення і впровадження відповідної бази даних, в якій будуть вказані судові рішення, які було винесено за аналогічними справами;

3) ускладнення або унеможливлення зміни права власності в судовому порядку з використанням незаконних схем рейдерських захоплень;

4) ведення чіткого обліку акцій підприємств із зазначенням власників і відстеженням історії їх змін;

5) унеможливлення передачі прав власності в короткі терміни, що, в свою чергу, зробить більш складним проведення рейдерських захоплень;

6) реалізація можливості відновлювання відповідних прав і статусу юридичної особи в разі доведення останнім незаконності реорганізації.

У разі, якщо зловмисники мають намір поглинання підприємства, у власника є час та можливості для своєчасного виявлення підготовлюваного заходу за характерними ознаками, а саме: позови міноритарних акціонерів до суду, зображення підприємства у СМІ з поганого боку, часті перевірки з боку державних органів, поява мітингувальників під стінами підприємства тощо.

Виявлено, що досліджені фактори дозволяють нівелювати ризики рейдерського захоплення підприємства. Їх використання значно ускладнює підготовку та збирання інформації зловмисниками, яку можна використати для подальшого нападу.

Врятуватися від рейдерського захоплення можна завдяки співпраці з досвідченими юристами та піарниками, які дадуть підприємцю можливість втримати контроль над власністю. Завдяки вказаним діям власник має змогу зберегти власне підприємство та захистити його від підготовлюваного нападу.

Жоден підприємець не застрахований від рейдерського нападу доти, доки на державному рівні не будуть прийняті заходи

для унеможливлення рейдерства. Серед можливих заходів: створення і впровадження відповідної бази даних, в якій будуть вказані подібні прецеденти по іншим підприємствам; створення і впровадження відповідної бази даних, в якій будуть вказані судові рішення, які було винесено за аналогічними справами; ускладнення або унеможливлення зміни права власності в судовому порядку з використанням незаконних схем; ведення чіткого обліку акцій підприємств з зазначенням власників і відстеженням історії їх змін; унеможливлення передачі прав власності в короткі терміни, що, в свою чергу, зробить більш складним проведення рейдерських захоплень; реалізація можливості відновлювання відповідних прав і статусу юридичної особи в разі доведення останнім незаконності реорганізації. Якщо заходи, які зазначено у роботі, будуть введені у дію, то проведення рейдерських захоплень буде надто складним, а, отже, невигідним.

Отже, жоден підприємець не застрахований від рейдерського нападу доти, доки на державному рівні не будуть прийняті заходи для унеможливлення рейдерства. Якщо заходи, які зазначено в роботі, будуть введені у дію, то проведення рейдерських захоплень буде надто складним, а, отже, невигідним.

9.4 ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БОРОТЬБИ З РЕЙДЕРСЬКИМИ ЗАХОПЛЕННЯМИ

Аудит інформаційної безпеки підприємства включає в себе комплексну перевірку всіх складових інформаційної системи підприємства. Ще він має назву в інших джерелах IT-аудит або аудит IT-інфраструктури.

Проблеми, які спонукають підприємства проводити аудит інформаційної безпеки підприємства:

– виявлені проблеми у роботі комп'ютерного та серверного обладнання;

DOI https://doi.org/10.36059/978-966-397-319-7-9

– відбувається трансформація структури підприємства та впровадження нових технологій;

– наявне застаріле програмне забезпечення та комп'ютерна техніка;

– наявні обмеження технічних можливостей підприємства;

– встановлено факт втрати інформації;

– зростання витрат на утримання ІТ-відділу;

– виявлені наявні загрози інформаційної безпеки.

Сутність аудиту інформаційної безпеки полягає в контролі за формуванням та збереженням диджитал бази з контролю за обігом інформації, виявлення зовнішніх та внутрішніх ризиків заволодіння інформації третіми особами, складання управлінської звітності з метою висловлення незалежної думки експерта-аудитора про її достовірність, законність, правильність, точність у всіх суттєвих аспектах, а також розробка пропозицій щодо попередження втрати даних та вдосконалення існуючої стратегії збереження документів.

Об'єктом аудиту інформаційної безпеки є процес перевірки несанкціонованого доступу до даних та надійного їх збереження.

Предметом аудиту інформаційної безпеки – політика інформаційної безпеки підприємства.

Метою аудиту інформаційної безпеки є висловлення незалежної думки експерта-аудитора про стан надійності збереження та доступу до даних, достовірність, законність, правильність, точність дотримання інформаційної гігієни співробітниками підприємства, а також розробка пропозицій щодо попередження можливих загроз цілісності масиву документів та оптимізації витрат на забезпечення та підвищення рівня захисту інформації.

Основні завдання аудиту інформаційної безпеки:

– забезпечити надійність збереження інформації;

– моніторити та запобігати несанкціонованому доступу до даних;

– перевірити достовірність, законність, правильність, точність дотримання інформаційної гігієни співробітниками підприємства;

– перевірити проведення інструктажів стосовно правил поводження з документами;

– визначити рівні допуску та належності до інформації у відповідних користувачів;

– розробити пропозиції щодо попередження можливих загроз цілісності масиву документів;

– актуалізація та підвищення ефективності управлінських рішень;

– забезпечити унеможливлення отримання неавторизованого доступу до інформації підприємства через вразливості IP-телефонії.

Аудит інформаційної безпеки підприємства є фундаментальною основою забезпечення стабільної та надійної роботи підприємства, яке при формуванні та обігу інформації долає різноманітні загрози в умовах нестабільної економіки та подій непереборної сили.

Надійна система інформаційної безпеки підприємства повинна надавати:

– надійність збереження інформації;

– запобігання несанкціонованому доступу до даних;

– підтримання інформаційної гігієни співробітників підприємства;

– засвоєння правил для співробітників стосовно поводження з документами;

– встановлення рівнів допуску та належності до інформації;

– попередження можливих загроз цілісності масиву документів.

Основні складові аудиту інформаційної безпеки підприємства:

1) аудит комп'ютерного та серверного обладнання;
2) аудит програмного забезпечення;
3) аудит засобів обміну інформації та зв'язку;
4) аудит використовуваних захисних систем;
5) аудит ефективності роботи відділу інформаційної безпеки.

Етапи аудиту інформаційної безпеки підприємства:

1) попередній етап;
2) фактичний етап;
3) основний етап;
4) заключний етап.

DOI https://doi.org/10.36059/978-966-397-319-7-9

Послідовність проведення аудиту інформаційної безпеки підприємства:

– перевірка забезпечення надійності збереження інформації;
– здійснення моніторингу захищеності даних підприємства;
– запобігання несанкціонованому доступу до даних;
– перевірка достовірності інформації, наявної на підприємстві;
– перевірка законності використання інформації;
– перевірка правильності заповнення та передачі документації;
– перевірка точності дотримання інформаційної гігієни співробітниками підприємства;
– перевірка дотримання розкладу та відвідування інструктажів стосовно правил поводження з документами;
– визначення рівнів допуску та належності до інформації у відповідних користувачів;
– перевірка якості та надійності використання антивірусного та антішпигунського програмного забезпечення;
– розробка пропозицій щодо попередження можливих загроз цілісності масиву документів;
– актуалізація та підвищення ефективності управлінських рішень;
– забезпечити унеможливлення отримання неавторизованого доступу до інформації підприємства через вразливості IP-телефонії.

Удосконалений механізм аудиту інформаційної безпеки підприємства (ІБП) наведено на рис. 9.4.

Удосконалено функції аудиту інформаційної безпеки підприємства:

1) оптимізаційна – розробка пропозицій до керівництва з питань вибору найкращих варіантів збереження інформації;

2) контрольна – перевірка дотримання правильності збереження документів;

3) захисна – захист інтересів підприємства щодо безпеки даних;

4) інформаційна – своєчасне повідомлення підприємств про ненадійну систему захисту;

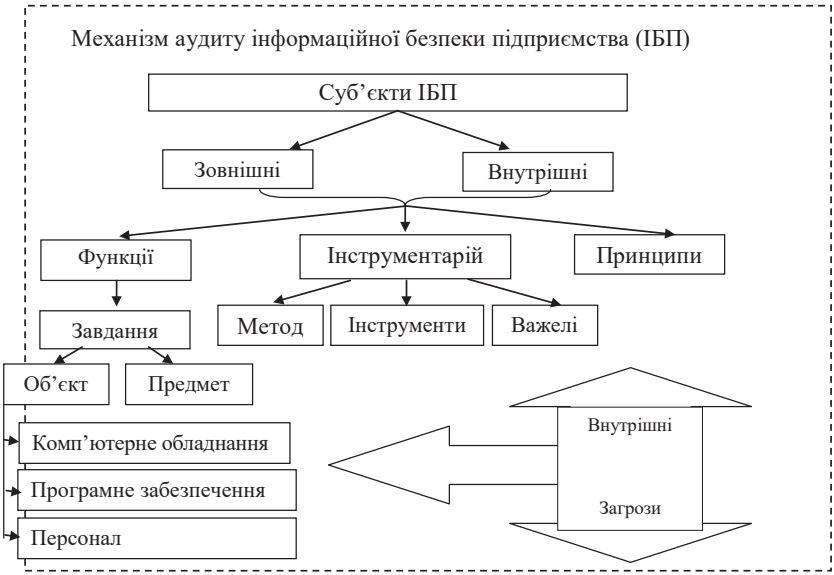


Рисунок 9.4 – Удосконалений механізм аудиту інформаційної безпеки підприємства

5) профілактична – своєчасне виявлення загроз втрати інформації;

6) інструктивна – проведення тренінгів з інформаційної гігієни;

7) запобіжна – запобігання витоку інформації;

8) стратегічна – розробка заходів реагування на виток інформації;

9) консультаційна – роз'яснення стосовно необхідності дотримання правил поводження з інформацією;

10) прогнозна – розробка плану забезпечення надійності документообігу;

11) оціночна – оцінювання можливих загроз інформаційної безпеки;

12) облікова – забезпечення своєчасного надходження, руху та виходу інформації;

DOI https://doi.org/10.36059/978-966-397-319-7-9

13) нормативна – перевірка використання авторитетних програмних застосунків;

14) експертна – проведення експертизи для встановлення достовірності даних у документах;

15) аналітична – вивчення та аналіз існуючих засобів інформаційної безпеки підприємства;

16) стримуюча – стримування імовірних загроз несанкціонованого доступу до даних підприємства.

Виходячи з вищезазначених функцій, можна зробити висновок, що весь функціонал інформаційної безпеки підприємства взаємопов'язаний між собою та однаково важливий для забезпечення збереження даних.

Удосконалено принципи інформаційної безпеки підприємства:

1. Принцип взаємозв'язку полягає в тому, що вихідна інформація з відділу повинна безпечно до отримувача.

2. Принцип миттєвого реагування, тобто швидкість відсічі виявленої загрози.

3. Принцип системності, тобто всі безпекові норми формуються у єдину систему.

4. Принцип планування, тобто розробка плану внутрішнього контролю інформаційної безпеки.

5. Принцип ефективності встановлює відповідність понесених витрат та отриманих результатів від побудови інформаційної безпеки підприємства.

6. Принцип всебічного охоплення під собою має на меті перевірку всіх масивів інформації.

7. Принцип наявності полягає в забезпечені наявності паперових або електронних документів на підприємстві.

8. Принцип захищеності формує систему заходів щодо забезпечення надійного зберігання інформації.

9. Принцип системності забезпечує побудову надійної політики інформаційної безпеки.

10. Принцип логістичного підходу декларує ієрархічну подачу документації від підлеглого до керівника.

11. Принцип відповідності полягає у дотриманні стандартів оформлення документації.

12. Принцип раціональності визначається в тому, щоб зробити вибірку необхідної кількості документів для повного висвітлення інформації.

13. Принцип альтернативності полягає у вивченні програмних застосунків, які на задовільному рівні забезпечують інформаційну безпеку підприємства.

14. Принцип інтегрованості складається в розробці окремих модулів та впровадження їх у існуючу систему попередження та уникнення загроз несанкціонованого доступу до даних.

15. Принцип законності полягає в дотриманні норм національного та міжнародного законодавства стосовно доступу до різного роду інформації.

16. Принцип економічності передбачає сталі зменшення видатків на отримання, обробку та передачу інформації.

17. Принцип координації дозволяє зв'язувати різні підрозділи між собою з метою підвищення їх ефективності.

18. Принцип безперервності передбачає постійну розробку та впровадження посиленого захисту інформації.

19. Принцип диференційованості дозволяє диференціювати захист інформації з огляду на її важливість.

20. Принцип гнучкості дозволяє швидко підлаштовуватись під зміну сучасної кіберзлочинності.

21. Принцип відповідальності полягає у призначенні відповідальних за захист даних підприємства.

22. Принцип компетенції означає наявність відповідної кваліфікації у співробітників відділу інформаційної безпеки підприємства.

23. Принцип зрозумілості полягає у доведенні до відома співробітників правил інформаційної гігієни.

24. Принцип достовірності означає, що вся інформація, яку отримають співробітники підприємства є однозначно достовірною.

25. Принцип своєчасності регламентує терміни підготовки інформації співробітниками підприємства.

DOI https://doi.org/10.36059/978-966-397-319-7-9

26. Принцип контролю полягає у постійному нагляді за використовуваними засобами захисту інформації та використання даних співробітниками.

27. Принцип попередження означає відвертання загрози у випадку великої її вірогідності.

28. Принцип конфіденційності забезпечує гарантоване збереження даних.

29. Принцип придатності показує рівень придатності комп'ютерного обладнання для забезпечення сучасного рівня захисту.

30. Принцип надійності гарантує застосування надійної та сучасної системи захисту інформації.

31. Принцип узгодженості дозволяє узгоджувати систему захисту між рівнями управління.

Отже, від дотримання принципів аудиту інформаційної безпеки залежить надійність використовуваної та захищеність зберігаємої інформації. Вищенаведені принципи будуть використані для оцінювання ефективності проведення аудиту інформаційної безпеки підприємства.

Переваги проведення аудиту інформаційної безпеки підприємства:

– отримання реальної оцінки стану захищеності інформації підприємства;

– забезпечення керівництва інформацією про придатність комп'ютерного обладнання;

– впевненість у надійності системи інформаційної безпеки на підприємстві;

– здійснити діагностику ефективності роботи служби інформаційної безпеки підприємства;

– підтримування актуальної версії резервної копії на захищеному просторі підприємства;

– забезпечення безперебійної роботи системи пошуку та видалення вірусів;

– впровадження обов'язкових вимог до змісту паролів та своєчасне їх оновлення;

– унеможливлення збоїв або виходу із ладу комп'ютерного обладнання у випадку перевантаження системи підприємства;

– проведення інвентаризації наявного обладнання та встановленого ПЗ;

– проведення оновлення ПЗ та модернізації комп'ютерного обладнання;

– проведення аналізу існуючих загроз через наявність недоліків у системі інформаційної безпеки;

– надання рекомендацій щодо покращення антивірусного захисту даних на підприємстві.

Види аудиту інформаційної безпеки підприємства, а саме: експрес-аудит, комплексний аудит, операційний аудит.

Анкету перевірки інформаційної безпеки підприємства подано в табл. 9.1 (див. с. 498). У програмі аудиту інформаційної безпеки підприємства відображені основні процедури для вирішення основних завдань аудиторської перевірки.

Одержавши в процесі попереднього планування дані про підприємство, аудитор приступає до розробки загального плану аудиту інформаційної безпеки підприємства (табл. 9.2, див. с. 498–499). План аудиту є документом організаційно-методологічного характеру та складається з переліку робіт на основних етапах аудиту і строків їх виконання із зазначенням джерел інформації. Аудит інформаційної безпеки підприємства авторами рекомендується проводити в кілька етапів.

При первісному аудиті, процедури аудиту будуть залежати від рівня довіри до результатів попереднього аудиту. Якщо аудит буде базуватися на даних попереднього аудиту, то необхідно уважно вивчити його робочі документи або детально опис інформаційної безпеки підприємства, чи адекватним був підхід попереднього аудитора.

Програму аудиту інформаційної безпеки підприємства наведено в табл. 9.3 (див. с. 499–500). Для вирішення поставлених завдань аудиту інформаційної безпеки підприємства пропонуємо робочі документи аудитора (табл. 9.4–9.8, див. с. 500–501), які на думку авторів стануть обґрунтованими доказами якісного проведення аудиту інформаційної безпеки підприємства.

DOI https://doi.org/10.36059/978-966-397-319-7-9

Таблиця 9.1 – Анкета перевірки інформаційної безпеки підприємства

№	Зміст питання	Варіанти відповіді			
		інформація відсутня	так	ні	примітки
1	Чи укладено договір про нерозголошення інформації?				
2	Чи обмежений доступ до сумнівних ресурсів?				
3	Чи проводяться інструктажі з інформаційної гігієни?				
4	Чи проводиться резервне копіювання даних підприємства?				
5	Чи були випадки несанкціонованого витоку інформації?				
6	Чи проводиться щорічна інвентаризація обладнання та ПЗ?				
7	Чи відбувається оновлення обладнання та/або ПЗ за результатами інвентаризації?				
8	Чи існують правила щодо форматів паролів?				
9	Чи існують обмеження на під'єднання сторонніх засобів до комп'ютерного обладнання підприємства?				
10	Чи відбувається регулярне оновлення антивірусного забезпечення?				

Таблиця 9.2 – Загальний план проведення інформаційної безпеки підприємства

Етап аудиторської перевірки	Аудиторські процедури	Аудиторські докази	Період проведення	Виконавці
1	2	3	4	5
Підготовчий	Знайомство з існуючою системою захисту інформації	Інструкції стосовно захисту інформації		
Фактичний	Проведення інвентаризації комп'ютерного обладнання та програмного забезпечення	Інвентаризаційний опис, Порівняльна відомість		

Закінчення таблиці 9.2

1	2	3	4	5
Основний	Перевірка дотримання інформаційної гігієни співробітниками підприємства	Журнали інструктажів		
	Перевірка правильності заповнення документації та її передачі	Первинні документи, Наказ про облікову політику, Графік документообігу		
	Перевірка рівнів допуску та належності до інформації у відповідних користувачів	Посадові інструкції		
Завершальний	Складання аудиторського звіту і висновку	Звіт		

Таблиця 9.3 – Програма аудиту інформаційної безпеки підприємства

№	Мета	Перелік аудиторських процедур	Критерії якості	Метод перевірки	Код робочого документа	Період проведення	Виконавець	Примітки
1	2	3	4	5	6	7	8	9
1	Впевнитись у фактичної наявності комп'ютерного обладнання та відповідності його даним бухгалтерії	Проведення інвентаризації комп'ютерного обладнання	А, Б, В, Г	Суцільний, фактичний	ІКП-1			
2	Впевнитись у фактичній наявності програмного забезпечення та відповідності його даним бухгалтерії	Проведення інвентаризації програмного забезпечення	А, Б, В, Г	Суцільний, фактичний	ІПЗ-2			
3	Впевнитись у точності дотримання	Перевірка дотримання інформаційної гігієни	А, Б, В, Г, Є	Вибірковий, фактичний	ІБП-3			

DOI https://doi.org/10.36059/978-966-397-319-7-9

Закінчення таблиці 9.3

1	2	3	4	5	6	7	8	9
	інформаційної гігієни співробітниками підприємства	співробітниками підприємства						
4	Впевнитись у правильності заповнення та передачі документації	Перевірка правильності заповнення документації та її передачі	А, Б, В, Г, Є	Вибірковий, формальний	ІБП-4			
5	Впевнитись у відповідності рівню допуску та належності до інформації у відповідних користувачів	Перевірка рівнів допуску та належності до інформації у відповідних користувачів	А, Б, В, Г, Є	Вибірковий, фактичний	ІБП-5			
Критерії якості аудиторської перевірки: наявність – А; правдивість – Б; права та зобов'язання – В; повнота – Г; вимірювання – Д; оцінка вартості – Е; подання і розкриття – Є.								

Таблиця 9.4 – Робочий документ аудитора
про інвентаризацію комп'ютерного обладнання

Вид комп'ютерного обладнання	Інвентарний номер	Матеріально-відповідальна особа	За даними бухгалтерії	За даними інвентаризації	Відхилення	Примітки

Таблиця 9.5 – Робочий документ аудитора про інвентаризацію
програмного забезпечення

Вид програмного забезпечення	Номер ліцензії	Матеріально-відповідальна особа	За даними бухгалтерії	За даними інвентаризації	Відхилення	Примітки

Таблиця 9.6 – Робочий документ аудитора з перевірки дотримання інформаційної гігієни співробітниками підприємства

ПІБ співробітника	Дата останнього інструктажу	Наявність зауважень	Наявність надійного паролю	Наявність доступу до мережі	Рівень доступу до комерційної інформації	Примітки

Таблиця 9.7 – Робочий документ аудитора з перевірки правильності заповнення та передачі документації

Вид первинного документу	Відповідальна особа за виписку	Наявність заповнення основних реквізитів						Термін виписки	ПІБ отримувача документа	Термін передачі	Примітки
		№	дата	кількість	сума	підпис	печатка				

Таблиця 9.8 – Робочий документ аудитора з перевірки рівнів допуску та належності до інформації у відповідних користувачів

ПІБ співробітника	Назва відділу	Посада	Рівень допуску відповідно до посади	Фактичний рівень допуску	Відхилення	Примітки

Отже, удосконалено аудит інформаційної безпеки підприємства, що на відміну від існуючих включає: анкету, загальний план аудиту, програму аудиту, робочі документи аудитора.

Запропонована методика проведення перевірки надасть змогу аудитору охопити всі аспекти перевірки інформаційної безпеки підприємства, дослідити правильність, своєчасність, законність їх відображення, вчасно виявити порушення, провести якісний аудит, попередити загрози та оптимізувати витрати підприємства.

DOI https://doi.org/10.36059/978-966-397-319-7-9

9.5 ЗДІЙСНЕННЯ АНАЛІЗУ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ НА ТОВ «ЗАПОРІЗЬКИЙ ЛИВАРНО-МЕХАНІЧНИЙ ЗАВОД» В СИСТЕМІ АУДИТУ МЕТОДІВ БОРОТЬБИ З ЗАГРОЗАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПІДВИЩЕННЯ ЙОГО ЕФЕКТИВНОСТІ

Українські підприємства сьогодні переживають не найкращі часи. Військова агресія рф проти України, обстріли та терор українських земель, понівечена війною українська економіка та промисловість. Тема роботи актуальна тому, що кожна цивілізована держава у світі повинна розуміти, що така біда може спіткати кожного, і потрібно знати, що робити про подібних ситуаціях.

Металургійна промисловість відіграє дуже значущу та велику роль у розвитку України. Завдяки неї, Україна здатна сама виробляти металургійну продукцію, оброблювати метали, створювати власні методики із виробництва у металургійній галузі та створювати нові зв'язки із іноземними партнерами для імпорту та експорту металів та металоконструкцій.

Аналіз господарської діяльності виконаний на підставі даних ТОВ «Запорізький ливарно-механічний завод», а саме досліджено: потенціал з виробництва, завантаження виробничих потужностей, продуктивність персоналу таких цехів, як: ливарний цех, механічний цех та металоконструкції.

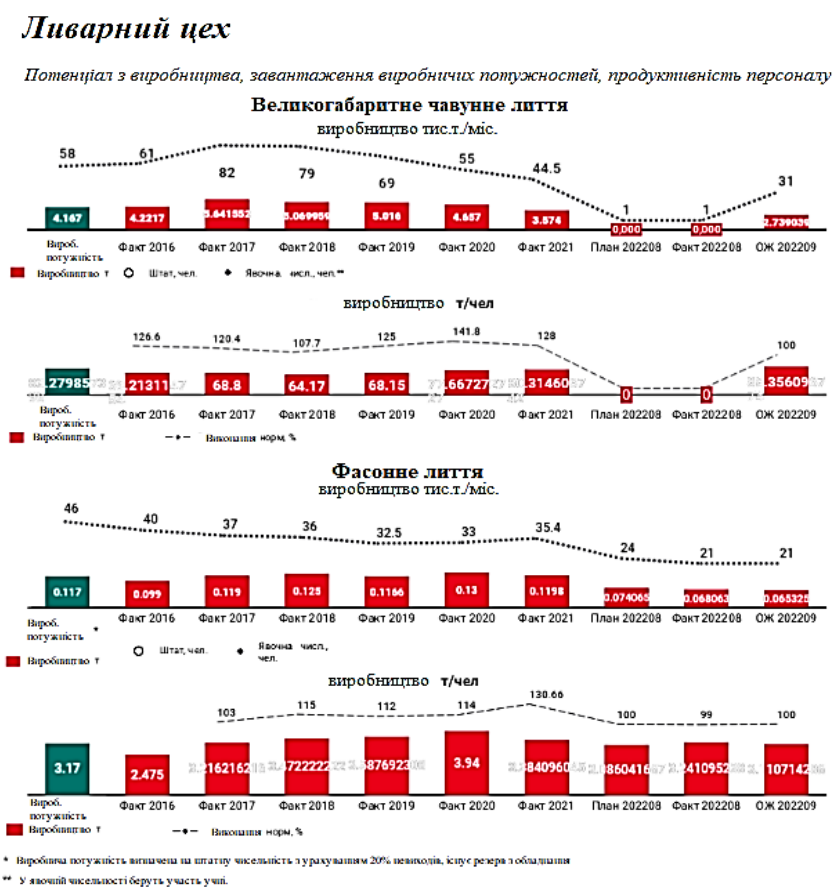
Результати аналізу ливарного цеху ТОВ «Запорізький ливарно-механічний завод» за 2022 р. наведено на рис. 9.5 (див. с. 503).

За результатами аналізу встановлено, що за великогабаритним чавунним литтям:

– простій відділення у серпні;

– очікуване виробництво у травні становитиме 2739 т. При плановій чисельності 31 людина, продуктивність становитиме 88 т/чол.

Тобто, при плануванні ми спостерігаємо значне зниження виробничих спроможностей підприємства через інтенсивні бойові дії та перебої із логістичним забезпеченням сировиною та матеріалами.



* Виробнича потужність визначена на штатну чисельність з урахуванням 20% невиходів, існує резерв з обладнання

** У явочній чисельності беруть участь учні.

Рисунок 9.5 – Результати аналізу роботи ливарного цеху ТОВ «Запорізький ливарн503о-механічний завод»

Результати аналізу роботи ливарного цеху ТОВ «Запорізький ливарно-механічний завод» за 2022 р. наведено на рис. 9.6 (див. с. 504).

За результатами аналізу встановлено, що по механічній обробці:

– виробництво у нормо-годинах за серпень 2022 р. склало 30,3 н.-год, що на 0,9 н.-год значення;

– перевиконання планових обсягів виробництва обумовлено освоєнням нових та додаткових видів продукції (пресуючий вузол,

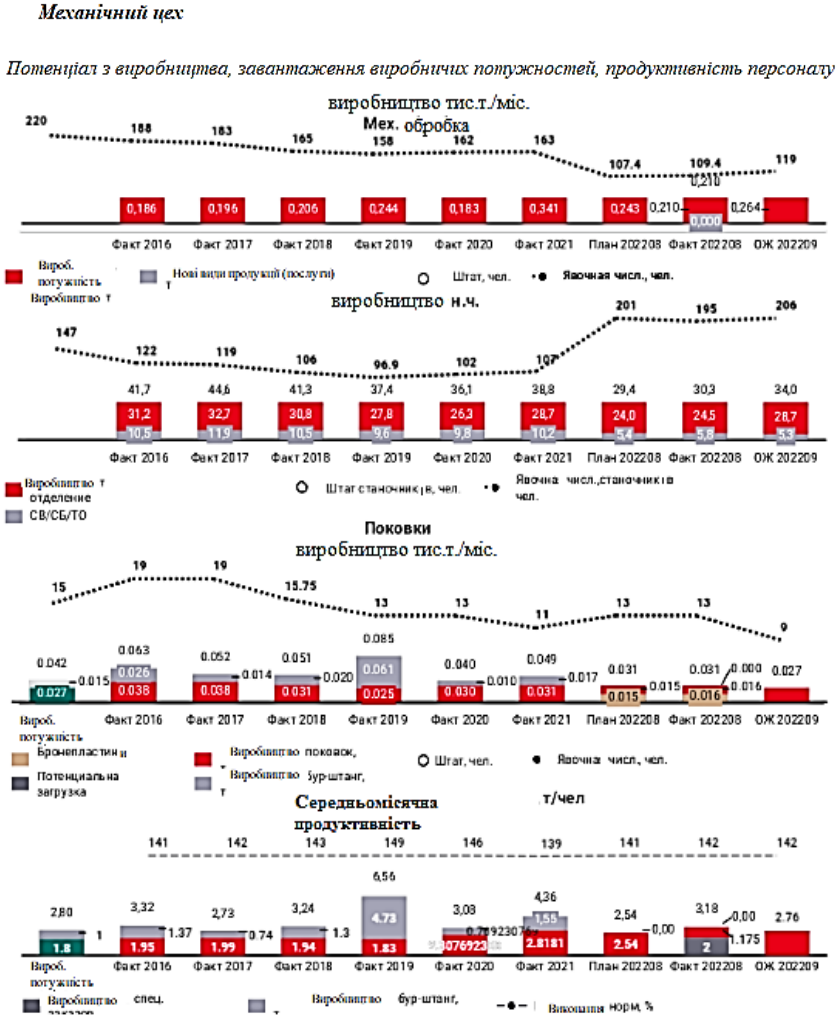


Рисунок 9.6 – Результати аналізу роботи механічного цеху ТОВ «Запорізький ливарно-механічний завод»

плити ЗКХЗ, послуга з нарізки зубів вал-шестерень, відновлення чаші та конуса засипного апарату доменної печі).

У вересні 2022 р. збільшення виробництва в тонах і нормогодинах за рахунок освоєння нових обсягів продукції у зв'язку із закриттям підприємств групи.

Також, слід зазначити, що через знаходження нових (альтернативних) європейських постачальників, підприємству можуть надаватися певні пільги та квоти.

Виконання виробничої програми з ковок (КВ) склало 15,5 т при плані 15,3 т, що складає 101,4 % заданого.

Результати аналізу роботи цеху металоконструкцій ТОВ «Запорізький ливарно-механічний завод» за 2022 р. наведено на рис. 9.7 (див. с. 506).

За результатами аналізу встановлено, що за цехом металоконструкції:

– виробництво металоконструкції (з урахуванням послуг з нових видів продукції) за серпень 2022 р. становило 260 т, що відповідає плановому значенню;

– скорочення виробництва продукції щодо 2021 р. пов'язано з відмовою від проведення низки капітальних ремонтів, а також коригуванням заявок замовника внаслідок зміни графіка роботи через проведення воєнних дій;

– очікуване виробництво у вересні становитиме 267 т за рахунок виготовлення металоконструкцій ШУ «Петровського» Копер (загальним обсягом 379 т), металоконструкцій ШУП Армування Рудстанок (загальним обсягом 45 т), Трубопроводів дегазації ШУП (загальною вагою 165 т) та металоконструкцій ЦГЗК (загальний обсяг 210 т), а також виготовлення металоконструкцій для ЗСУ (20 шт. модульних укриттів вагою 44 т).

Підводячи підсумок із дослідження продуктивності виробництва цехів можна сказати, що виконується велика робота задля безперебійної роботи підприємства та всебічної допомоги ЗСУ при боротьбі із російською агресією.

Для проведення дослідження про визначення витратного коефіцієнту металу, використовуємо вхідні дані підприємства, які наведені в табл. 9.9–9.10 (див. с. 507–508).

DOI https://doi.org/10.36059/978-966-397-319-7-9

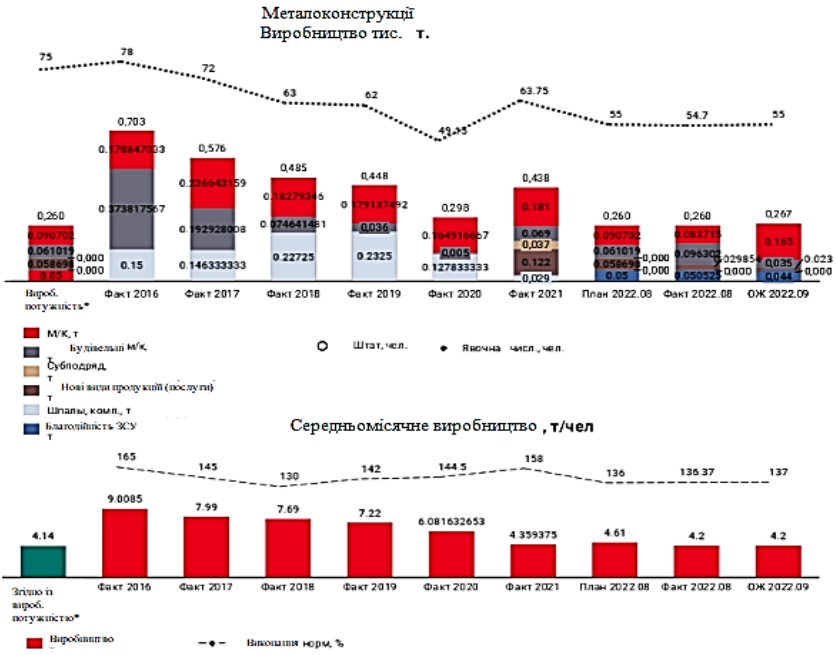
За табл. 9.9 спостерігаємо, що при кожній певній позиції по даним – факт відповідає нормативу.

За табл. 9.10 бачимо, що при певній позиції спостерігається зменшення (сталеве й бронзове лиття) та збільшення (лиття марочного чавуну) витрат через різні фактори, що сприяють виробництву на підприємстві. Ефект впливу факторів на балансовий прибуток наведено на рис. 9.8 (див. с. 509).

Разом ефект обсягів та структури змін на $103,1 тис., у т. ч. ефект від обсягів реалізації $610,1 тис.

Металоконструкції

Потенціал з виробництва, завантаження виробничих потужностей, продуктивність персоналу



*Вироб. потужність на квітень 2022р. розрахована на штатну чисельність з урахуванням 15,5% невиходів та простою 50% відрядників, існує резерв по обладнанню. З урахуванням освоєння нових послуг виробнича потужність становить 173 т (150 т виготовлення).

** З 2020 року збільшилася трудомісткість виготовлення м/к, порівняно з попередніми періодами, виключено компенсатори, зменшено обсяг шпал.

Рисунок 9.7 – Результати аналізу роботи цеху металоконструкцій ТОВ «Запорізький ливарно-механічний завод»

Таблиця 9.9 – Аналіз відхилення від нормативу витратного коефіцієнта металу цеху металоконструкцій

Позиція	Здача, т	Вплив на РКМ, %	ZBB	Норматив	Факт	Відхилення, %	Пояснення
По цеху	151,246	—	—	1,373	1,372	−0,07	Факт відповідає нормативу
М/к чорні без сварки	27,088	17,91 %	1,148	1,151	1,150	−0,05	Факт відповідає нормативу
М/к чорні сварні	71,131	47,03 %	1,092	1,104	1,096	−0,7	Факт відповідає нормативу
М/к чорн. св. Копер	40,04	26,47 %	—	1,289	1,289	0	Факт відповідає нормативу

Таблиця 9.10 – Аналіз відхилення від нормативу витратного коефіцієнта металу ливарного цеху

Позиція	Здача, т	Вплив на РКМ, %	ZBB	Норматив	Факт	Відхилення, %	Пояснення
1	2	3	4	5	6	7	8
ОПКСО							
Великогабаритне чавунне лиття	0	—	1,061	—	—	—	Виробництва не було
ОПФЛ							
Сталеве лиття	35,029	58,4	1,194	2,158	2,030	−5,9	Зменшення витрати рідкої сталі на виробництво сталевого лиття через зміну фактично виробленого сортаменту порівняно із плановим: заплановано виробництво сталевого лиття

Закінчення таблиці 9.10

1	2	3	4	5	6	7	8
							з виходом придатного 46,3 %, фактично – 49,3 %
Лиття із марочного чавуну	15,905	26,5	1,095	1,147	1,224	+6,7	Збільшення витрати рідкого чавуну на чавунне лиття з марочного чавуну з причин: проведення плавок ЧХ1 в 3-т тиглі в мінімально можливому обсязі, що перевищує ємність 1-т тигля для виконання плана виробництва підових плит на замовлення 59-403/95; збільшеного утворення відходів через проведення повноцінної плавки в повному обсязі укомплектованої формами під заливку, виходячи з умови якісної заливки плит 59-403/95, відсутність інших замовлень для комплектації плавки (плавка 4-139, тигель 3-т)
Бронзове лиття	9,008	15,0	1,321	1,645	1,446	−12,1	Зменшення витрати рідкої бронзи на виробництво кольорового лиття через зміну фактично виробленого сортаменту порівняно із плановим: заплановано виробництво сталевого лиття з виходом придатного 60,8 %, фактично – 69,2 %

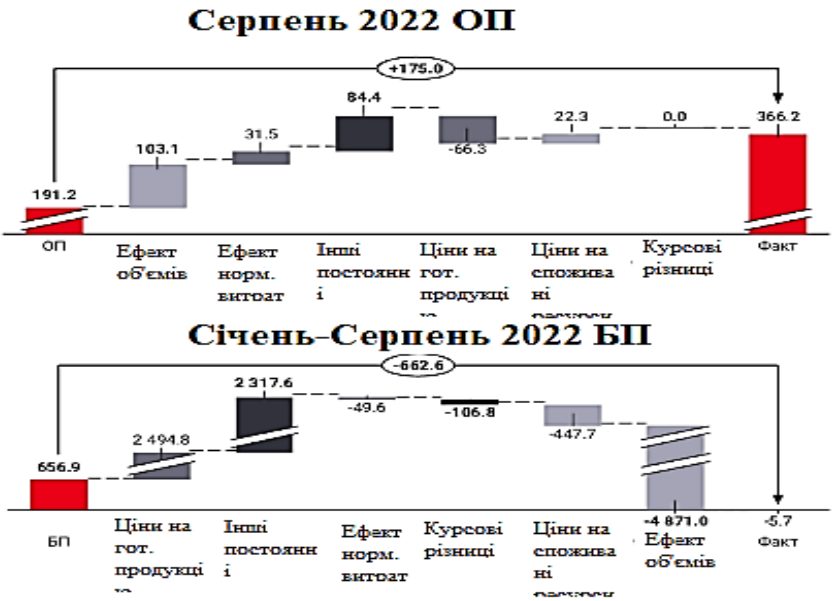


Рисунок 9.8 – Ефект впливу факторів на балансовий прибуток

Основне відхилення прибутку за цехами:

– у реалізації ливарного цеху $47,1 тис., зокрема основне відхилення: $56,6 тис., збільшення реалізації продукції на адресу ЗВТ на 19 т;

– у реалізації механічного цеху $206,4 тис., а саме відхилення обумовлено збільшенням реалізації деталей з хутра. обробкою на 6,5 т;

– у реалізації цеху металоконструкцій $356,6 тис., причому відхилення обумовлено позаплановим відвантаженням 11,8 т будівельних металоконструкцій;

– ефект витрат сировини та витрат на виробництво $(150,1) тис., основною причиною є відсутність обсягів виробництва, а також зниження обсягів виробництва на 20,6 т;

– ефект зміни складу готової продукції на $(385,9) тис., а сама зниження реалізації у зв'язку з військовим становищем, реалізація буде проводиться в наступних періодах;

– ефект зміни інших змінних витрат на $29,0 тис. за рахунок зниження витрат за іншими змінних послуг.

Встановлено, що норми витрат збільшились на $31,5 тис., у тому числі основними факторами змін є:

– збільшення питомих витрат на $(5,4) тис., у т. ч.:

– збільшення витрат на природний газ виробництва фасонного лиття обумовлено доопрацюванням продукції, що перебувала у незавершеному виробництві минулих періодів на $(8,5) тис.;

– зниження електроенергії за рахунок зміни асортименту продукції, що дозволило комплектувати повноцінні плавки на $3,6 тис.;

– збільшення інших енергетичних ресурсів $(0,5) тис.;

– зниження витрат за основною сировиною на $36,9 тис., у т. ч.: за цехом металоконструкцій $12,2 тис. покупного металу в зв'язку з економією в 10 кг/т за основною калькуляцією (чорна зварна) та економія в 42 кг/т на тендерне замовлення (1,247 за фактом замість 1,289 у плані);

– у ливарному цеху зменшено на $18,2 за іншими допоміжними матеріалами у зв'язку із збільшенням використання зливків власного виробництва.

Помісячне виконання прибутку за ключовими драйверами наведено у табл. 9.11.

Таблиця 9.11 – Помісячне виконання прибутку за ключовими драйверами

Показник		**Січень-лютий**	**Березень**	**Квітень-серпень**	**8 міс.**
Тис. дол.	Факт. EBITDA	41,35	−1065,1	646,9	−5,7
Тис. дол.	Витрати, пов'язані із воєнним положенням	2,9	82,5	523,1	508,5
Тис. дол.	EBITDA без обліку неконтролюючих факторів	416,4	−983,6	1170,0	602,8
Тис. дол.	Прибуток EBITDA	230,9	45,7	842,2	667,0
Тис. дол.	Відхилення прибутку EBITDA без обліку неконтролюючих факторів	647,4	−1029,3	327,8	−54,1

За табл. 9.11 бачимо, що при використанні показника EBIDTA у розділах «EBITDA без обліку неконтролюючих факторів» та «Відхилення БП EBITDA без обліку неконтролюючих факторів» у період місяців січень-лютий та квітень-серпень спостерігається значне збільшення прибутку. У березні місяці у тих же розділах відбувається зменшення прибутку. А в розділі «EBITDA без обліку неконтролюючих факторів» за 8 місяців відбувається збільшення прибутку, але у «Відхилення прибутку EBITDA без обліку неконтролюючих факторів» навпаки спостерігається його зменшення.

Компанія Метінвест об'єднає три ливарно-механічних заводів в єдиний комплекс, який розташований в Запоріжжі, Кривому Розі та Кам'янському. Таке об'єднання надасть багато переваг, а саме знизяться витрати на виробництва та управління, а значить підвиситься прибуток та збільшиться ефективність господарської діяльності.

Анкету аудиту методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності подано в табл. 9.12 (див. с. 512).

Одержавши в процесі попереднього планування дані про підприємство, аудитор приступає до розробки загального плану аудиту методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності (табл. 9.13, див. с. 513).

Програму аудиту методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності наведено в табл. 9.14 (див. с. 514).

Для вирішення поставлених завдань аудиту методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності пропонуємо робочі документи аудитора (табл. 9.15–9.19, див. с. 515), які на думку авторів стануть обґрунтованими доказами якісного проведення аудиту.

Пропозиції щодо удосконалення господарської діяльності ТОВ «Запорізький ливарно-механічний завод»:

– залучення іноземних інвестицій;
– участь у міжнародних програмах та грантових проєктах;

DOI https://doi.org/10.36059/978-966-397-319-7-9

– залучення адміністративних відділів підприємства в отриманні прибутку шляхом надання послуг;
– економія витрат адміністративними відділами підприємства;

Таблиця 9.12 – Анкета аудиту методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності

№	Зміст питання	Варіанти відповіді			
		інформація відсутня	так	ні	примітки
1	Чи використовуєте ви власні розробки для виявлення загроз?				
2	Чи є у вас окремий підрозділ для виявлення та боротьби з загрозами?				
3	Як часто виконується перевірка на наявність прихованих загроз: – раз на день; – раз на декілька днів; – раз на тиждень; – раз на місяць?				
4	Чи був встановлений раніше виток інформації з підприємства?				
5	Чи були помічені співробітники під час спроб викрадення комерційної інформації?				
6	Як часто відбуваються збої в інформаційній системі підприємства: – раз на день; – раз на декілька днів; – раз на тиждень; – раз на місяць?				
7	Як часто відбуваються оновлення програмного забезпечення для унеможливлення шпигунської діяльності на підприємстві: – раз на декілька днів; – раз на тиждень; – раз на декілька тижнів; – раз на місяць; – раз у квартал; – раз у півріччя; – раз на рік?				

– залучення до співпраці ливарного заводу SOBOWIDZ, м. Гданськ, Польща;

– залучення науковців до розробок сучасних матеріалів та технологій виробництва, які необхідні у воєнний період для подолання російської агресії в Україні;

– залучення науковців до розробок сучасних матеріалів та технологій виробництва, які необхідні у післявоєнний період для відновлення інфраструктури та розбудови України. Це надасть збільшення прибутку та підвищення ефективності діяльності підприємства.

Таблиця 9.13 – Загальний план аудиту методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності

Етап аудиторської перевірки	**Аудиторські процедури**	**Аудиторські докази**	**Період проведення**	**Виконавці**
Підготовчий	Знайомство з існуючими методами боротьби з загрозами інформаційної безпеки	Інструкції з підтримання безпеки підприємства		
	Аналіз господарської діяльності	Результати аналізу		
Фактичний	Перевірка останньої дати оновлення програмного забезпечення	Встановлені версії програмного забезпечення, Інструкції щодо встановленого програмного забезпечення, Інвентаризаційні описи, Порівняльні відомості		
	Перевірка встановленого обсягу програмного забезпечення			
Основний	Перевірка відповідності витрат встановленим нормам	Встановлені на підприємстві дані щодо норм витрат		
	Перевірка відповідності витратного коефіцієнта встановленим нормам	Встановлені на підприємстві дані щодо норм витратного коефіцієнту		
	Перевірка відповідності прибутку встановленому плану	Встановлений на підприємстві план прибутку		
Завершальний	Складання аудиторського звіту і висновку	Звіт		

Таблиця 9.14 – Програма аудиту методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності

№	Мета	Перелік аудиторських процедур	Критерії якості	Метод перевірки	Код робочого документа	Період проведення	Виконавець	Примітки
1	Впевнитись у наявності надійної системи захисту	Перевірка останньої дати оновлення програмного забезпечення	А, Б, В	Вибірковий, фактичний	ДМБ-1			
2	Впевнитись у повноті встановленого програмного забезпечення та його відповідності інструкції	Перевірка встановленого обсягу програмного забезпечення	А, Б, В, Г	Вибірковий, фактичний	ДМБ-2			
3	Впевнитись у відповідності витрат встановленим нормам	Перевірка відповідності витрат встановленим нормам	А, Б, В, Г	Суцільний, документальний, арифметичний	ДМБ-3			
4	Впевнитись у відповідності витратного коефіцієнта встановленим нормам	Перевірка відповідності витратного коефіцієнта встановленим нормам	А, Б, В, Г	Суцільний, документальний, арифметичний	ДМБ-4			
5	Впевнитись у відповідності прибутку встановленому плану	Перевірка відповідності прибутку встановленому плану	А, Б, В, Г, Є	Суцільний, документальний, арифметичний	ДМБ-5			
Критерії якості аудиторської перевірки: наявність – А; правдивість – Б; права та зобов'язання – В; повнота – Г; вимірювання – Д; оцінка вартості – Е; подання і розкриття – Є.								

Таблиця 9.15 – Робочий документ аудитора з перевірки останньої дати оновлення програмного забезпечення

Назва комп'ютерного обладнання	Назва програмного забезпечення	Термін, в який повинно бути оновлено ПЗ	Фактичний термін оновлення ПЗ	Відхилення	Примітки

Таблиця 9.16 – Робочий документ аудитора з перевірки встановленого обсягу програмного забезпечення

Назва комп'ютерного обладнання	ПЗ, яке повинно бути встановлено згідно з інструкцією	Версія програмного забезпечення	Фактично встановлено ПЗ	Відхилення	Примітки

Таблиця 9.17 – Робочий документ аудитора з перевірки відповідності витрат встановленим нормам

Підрозділ	Елемент витрат	Норми витрат	Фактичні витрати	Відхилення	Примітки

Таблиця 9.18 – Робочий документ аудитора з перевірки відповідності витратного коефіцієнта встановленим нормам

Підрозділ	Вид продукції	Норми витратного коефіцієнта	Фактичний витратний коефіцієнт	Відхилення	Примітки

Таблиця 9.19 – Робочий документ аудитора з перевірки відповідності прибутку встановленому плану

Підрозділ	Вид прибутку	Планові норми прибутку	Фактичний прибуток	Відхилення	Примітки

DOI https://doi.org/10.36059/978-966-397-319-7-9

Удосконалено аудит методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності, що на відміну від існуючих включає: анкету, загальний план аудиту, програму аудиту, робочі документи аудитора. Запропонована методика проведення перевірки надасть змогу аудитору охопити всі аспекти перевірки методів боротьби з загрозами інформаційної безпеки, дослідити правильність, відповідність, законність їх відображення, вчасно виявити порушення, провести якісний аудит, попередити загрози, оптимізувати витрати та прибутки підприємства, а також підвисити ефективність діяльності.

Передумовою забезпечення інформаційної безпеки підприємства є прийняття ефективних управлінських рішень у системі проведення аудиту інформаційної безпеки, що базуються на своєчасному запобіганні, виявленні, оцінюванні впливу інформаційної захищеності на господарську діяльність та подоланні ризиків зламу та викрадання даних.

Зростання інтересу до розгляду проблеми впливу аудиту інформаційної безпеки на інформаційну захищеність підприємства зумовлено необхідністю підвищення рівня якості та ефективності контролю за дотриманням інформаційної гігієни, виходячи з оцінки доцільності проведення зовнішнього та внутрішнього аудиту безпеки даних, а також удосконалення захисту.

Загроза інформаційної безпеки підприємства може виникати через збіг суб'єктивних (ведення неефективних заходів інформаційної безпеки) та об'єктивних (велика кількість хакерських або DDoS-атак) факторів.

Від ефективності проведення внутрішнього та зовнішнього аудиту інформаційної безпеки залежить і його результат. Підприємство повинно зіставляти отримані вигоди та понесені витрати на перевірку захищеності даних підприємства. Однак досліджені нами підприємства не проводять таких розрахунків перед початком аудиту інформаційної безпеки. Розроблена система показників для оцінювання ефективності інформаційної безпеки та аудиту захищеності даних базується на сформованих

нами принципах оцінювання якості й ефективності аудиту унеможливлення зламу як складової інформаційної безпеки та досліджень з економічної ефективності господарської діяльності підприємств.

Е. Дж. Долан та Д. Ліндсей зазначають, що необхідно розрізняти зовнішні та внутрішні витрати на виробництво продукції. Повні витрати (економічні витрати), крім витрат на виробництво (бухгалтерських витрат), включають нормальний прибуток як мінімальну величину, при одержанні якої є сенс займатися підприємницькою діяльністю.

На сьогодні в науковій літературі тривають дискусії щодо різних аспектів ефективності аудиту. Основні проблеми розкрито в працях таких аудиторів та вчених, як: А. Висоцький, І. Дмитренко, О. Долгова, С. Зубілевич, В. Труш, Л. Церетелі, М. Щірба та ін. Проте треба зауважити, що в цих джерелах хоч і наголошується на важливості оцінювання ефективності функціонування системи внутрішнього контролю, але економічні показники оцінювання не розраховуються.

При здійсненні господарської діяльності підприємства несуть бухгалтерські та економічні витрати. Тобто формула розрахунку бухгалтерських витрат ($В_{Ба}$) має такий вигляд:

$$В_{Ба} = В_{М} + В_{ЗА} + В_{ВІДР} + В_{А} + В_{ІН}, \qquad (9.1)$$

де $В_{Ба}$ – бухгалтерські витрати на аудит інформаційної безпеки, грн/рік;

$В_{М}$ – матеріальні витрати на проведення аудиту інформаційної безпеки, грн/рік;

$В_{ЗА}$ – витрати на оплату праці робітників з проведення аудиту інформаційної безпеки, грн/рік;

$В_{ВІДР}$ – витрати на соціальні заходи із заробітної плати робітників з проведення аудиту інформаційної безпеки, грн/рік;

$В_{А}$ – витрати на амортизацію обладнання з проведення аудиту інформаційної безпеки, грн/рік;

$В_{ІН}$ – інші витрати на проведення аудиту інформаційної безпеки, грн/рік.

DOI https://doi.org/10.36059/978-966-397-319-7-9

Економічні витрати, крім бухгалтерських, додатково включають частину нормативного прибутку підприємства, формула запису яких має вигляд:

$$В_{Еа} = В_{Ба} + П_Н, \quad (9.2)$$

де $В_{Еа}$ – економічні витрати з аудиту інформаційної безпеки, грн/рік;

$П_Н$ – нормативний прибуток з проведення аудиту інформаційної безпеки, грн/рік.

Нормативний прибуток від проведення аудиту інформаційної безпеки визначається добутком:

$$П_Н = В_{Ба} \times Е_{На}, \quad (9.3)$$

де $Е_{На}$ – нормативний показник абсолютної економічної ефективності бухгалтерських витрат на аудит інформаційної безпеки.

Показник нормативної ефективності від проведення аудиту інформаційної безпеки можна взяти на рівні нормативної рентабельності продукції:

$$Е_{На} \geq Р_Н, \quad (9.4)$$

де $Р_Н$ – нормативна рентабельність продукції.

Нормативна рентабельність продукції визначається відношенням нормативного прибутку до бухгалтерських витрат підприємства (ВБ):

$$Р_Н = \frac{П_Н}{В_Б}. \quad (9.5)$$

Методи оцінювання ефективності внутрішнього аудиту інформаційної безпеки підприємства включає розрахунок показників абсолютної, порівняльної економічної ефективності та економічного ефекту від проведення внутрішнього аудиту інформаційної безпеки для обґрунтування управлінських рішень.

Абсолютна економічна ефективність щодо бухгалтерських витрат на внутрішній аудит інформаційної безпеки визначається за формулою:

$$E'_{ва} = \frac{\Delta Д_{ва}}{В_{Ева}} \geq E'_{Нва}, \quad (9.6)$$

де $E'_{ва}$ – показник абсолютної економічної ефективності щодо бухгалтерських витрат на внутрішній аудит інформаційної безпеки, од.;

$\Delta Д_{ва}$ – додатковий результат, отриманий за рахунок внутрішнього аудиту інформаційної безпеки, грн/рік;

$В_{Ева}$ – бухгалтерські витрати на внутрішній аудит інформаційної безпеки, грн/рік;

$E'_{Нва}$ – нормативний показник абсолютної економічної ефективності бухгалтерських витрат на внутрішній аудит інформаційної безпеки, од.

Отже, найкращим варіантом проведення внутрішнього аудиту інформаційної безпеки буде той, у якого показник економічної ефективності щодо бухгалтерських витрат на внутрішній аудит інформаційної безпеки буде більшим від нормативного показника абсолютної економічної ефективності бухгалтерських витрат на внутрішній аудит інформаційної безпеки.

Абсолютна економічна ефективність щодо економічних витрат на внутрішній аудит інформаційної безпеки становитиме:

$$E'_{ва} = \frac{\Delta Д_{ва}}{В_{Ева}} \geq E'_{Нва}, \quad (9.7)$$

де $E'_{ва}$ – показник абсолютної економічної ефективності щодо економічних витрат на внутрішній аудит інформаційної безпеки, од.;

$В_{Ева}$ – економічні витрати на внутрішній аудит інформаційної безпеки, грн/рік;

$E'_{Нва}$ – нормативний показник абсолютної економічної ефективності економічних витрат на внутрішній аудит інформаційної безпеки, од.

Найкращим варіантом проведення внутрішнього аудиту інформаційної безпеки буде той, у якого показник економічної ефективності щодо економічних витрат на внутрішній аудит

DOI https://doi.org/10.36059/978-966-397-319-7-9

інформаційної безпеки буде більшим від нормативного показника абсолютної економічної ефективності економічних витрат на внутрішній аудит інформаційної безпеки.

Порівняльна економічна ефективність бухгалтерських витрат на внутрішній аудит інформаційної безпеки передбачає перевищення індексу результату над індексом витрат:

$$E_{Пва} = \frac{ІД_{ва}}{I_{ВБва}} > 1, \quad (9.8)$$

де

$$I_{Два} = \frac{\Delta Д_{ва2}}{\Delta Д_{ва1}}, \quad (9.9)$$

$$I_{ВБва} = \frac{В_{Бва2}}{В_{Бва1}} \quad (9.10)$$

тобто

$$E_{Пва} = \frac{\frac{\Delta Д_{ва2}}{\Delta Д_{ва1}}}{\frac{В_{Бва2}}{В_{Бва1}}} \geq 1, \quad (9.11)$$

де $E_{Пва}$ – показник порівняльної економічної ефективності бухгалтерських витрат на внутрішній аудит інформаційної безпеки, од.;

$\Delta Д_{ва1}$, $\Delta Д_{ва2}$ – додатковий результат, одержаний за рахунок внутрішнього аудиту інформаційної безпеки у базисному та новому періодах, грн/рік;

$I_{Два}$ – індекс додаткового результату, одержаного за рахунок внутрішнього аудиту інформаційної безпеки, од.;

$В_{Бва1}$, $В_{Бва2}$ – бухгалтерські витрати на внутрішній аудит інформаційної безпеки у базисному та новому періодах, грн/рік;

$I_{ВБва}$ – індекс бухгалтерських витрат на внутрішній аудит інформаційної безпеки, од.

Отже, найкращим варіантом проведення внутрішнього аудиту інформаційної безпеки буде той, у якого показник абсолютної економічної ефективності бухгалтерських витрат

на внутрішній аудит інформаційної безпеки буде максимальним ($Е_{Пва} = max$). При порівнянні двох варіантів кращим варіантом буде той, у якого індекс додаткового результату, одержаного за рахунок внутрішнього аудиту інформаційної безпеки, перевищує індекс бухгалтерських витрат на внутрішній аудит інформаційної безпеки.

Порівняльна економічна ефективність економічних витрат на внутрішній аудит інформаційної безпеки становитиме:

$$Е'_{Пва} = \frac{І Д_{ва}}{І_{ВЕва}} > 1, \quad (9.12)$$

де

$$І_{ВЕва} = \frac{В_{Ева2}}{В_{Ева1}} \quad (9.13)$$

тобто

$$Е'_{Пва} = \frac{\frac{\Delta Д_{ва2}}{\Delta Д_{ва1}}}{\frac{В_{Ева2}}{В_{Ева1}}} > 1, \quad (9.14)$$

де $Е'_{Пва}$ – показник порівняльної економічної ефективності економічних витрат на внутрішній аудит інформаційної безпеки, од.;

$В_{Ева1}$, $В_{Ева2}$ – економічні витрати на внутрішній аудит інформаційної безпеки у базисному та новому періодах, грн/рік;

$І_{ВЕва}$ – індекс економічних витрат на внутрішній аудит інформаційної безпеки, од.

Найкращим варіантом проведення внутрішнього аудиту інформаційної безпеки буде той, у якого показник абсолютної економічної ефективності економічних витрат на внутрішній аудит інформаційної безпеки буде максимальним ($Е'_{Пва} = max$). При порівнянні двох варіантів кращим варіантом буде той, у якого індекс додаткового результату, одержаного за рахунок внутрішнього аудиту інформаційної безпеки, перевищує індекс економічних витрат на внутрішній аудит інформаційної безпеки.

DOI https://doi.org/10.36059/978-966-397-319-7-9

Річний економічний ефект від проведення внутрішнього аудиту інформаційної безпеки можна розрахувати як різницю між одержаним результатом та додатковими витратами:

$$\Delta W_{ва} = \left(\Delta Д_{ва2} - \Delta Д_{ва1}\right) \times \left(\frac{В_{Ева1}}{\Delta Д_{ва1}}\right) - \left(В_{Ева2} - В_{Ева1}\right), \qquad (9.15)$$

де $\Delta W_{ва}$ – річний економічний ефект від проведення внутрішнього аудиту інформаційної безпеки, грн/рік.

Тобто найкращим варіантом проведення внутрішнього аудиту інформаційної безпеки підприємства буде той, у якого економічний результат від проведення внутрішнього аудиту буде більшим від додаткових витрат на одержання економічного результату від його проведення. Запропоновані показники для розрахунку економічної ефективності витрат на внутрішній аудит інформаційної безпеки підприємства подано в табл. 9.20 (див. с. 523).

Забезпечення прибутковості функціонування підприємства передбачає перевищення виручки від реалізації продукції над витратами на її виробництво. Це означає, що заходи стосовно забезпечення інформаційної безпеки підприємства також повинні бути ефективними. Визначення економічної ефективності інформаційної безпеки підприємства спрямовано на розрахунок відношення економічного результату до витрат живої та уречевленої праці та порівняння його з нормативним значенням.

На сьогодні економічну ефективність інформаційної безпеки підприємства визначають:

$$ЧФК = \frac{З_{від}}{В + З_{заг}}, \qquad (9.16)$$

де ЧФК – частковий функціональний критерій інформаційної безпеки підприємства;

$З_{від}$ – сукупний відвернений збиток за складовою;

В – сумарні витрати на реалізацію заходів щодо запобігання збиткам із цієї функціональної складової інформаційної безпеки підприємства в періоді, що аналізується;

$З_{заг}$ – загальний зазнаний збиток за цією функціональною складовою інформаційної безпеки підприємства.

Таблиця 9.20 – Удосконалена система показників економічної ефективності витрат на внутрішній аудит інформаційної безпеки підприємства

Вид економічної ефективності	Результати	Витрати	Показники економічної ефективності	Критерії
Абсолютна економічна ефективність витрат	$\Delta Д_{ва}$	$В_{Бва}$	$E_{ва} = \frac{\Delta Д_{ва}}{В_{Бва}}$	$\geq E_{Нва}$
	$\Delta Д_{ва}$	$В_{Ева}$	$E'_{ва} = \frac{\Delta Д_{ва}}{В_{Ева}}$	$\geq E'_{Нва}$
Порівняльна економічна ефективність витрат	$I_{Два} = \frac{\Delta Д_{ва2}}{\Delta Д_{ва1}}$	$I_{ВБва} = \frac{В_{Бва2}}{В_{Бва1}}$	$E_{Пва} = \frac{\frac{\Delta Д_{ва2}}{\Delta Д_{ва1}}}{\frac{В_{Бва2}}{В_{Бва1}}}$	>1
	$I_{Два} = \frac{\Delta Д_{ва2}}{\Delta Д_{ва1}}$	$I_{ВБва} = \frac{В_{Бва2}}{В_{Бва1}}$	$E'_{Пва} = \frac{\frac{\Delta Д_{ва2}}{\Delta Д_{ва1}}}{\frac{В_{Ева2}}{В_{Ева1}}}$	>1

Такий методичний підхід порушує один із важливих принципів побудови показника економічної ефективності, який означає, що витрати є причиною, а результати – наслідком цих витрат.

Пропонуємо розрахунок показника абсолютної економічної ефективності формування інформаційної безпеки підприємства здійснювати за формулою:

$$E_i = \frac{\Delta З}{В_i} > E_{і.н.}, \quad (9.17)$$

де E_i ($E_{і.н.}$) – показник (нормативний показник) абсолютної економічної ефективності формування інформаційної безпеки підприємства, відносні од.;

$\Delta З$ – відвернений збиток, одержаний за рахунок формування інформаційної безпеки підприємства, грн/рік;

$В_і$ – економічні витрати на формування інформаційної безпеки підприємства, грн/рік.

Критерієм ефективності показника абсолютної економічної ефективності є перевищення (рівність) його нормативного значення. Ми вважаємо, що нормативним значенням повинна бути одиниця $Е_{н.\,і.}=1$. Тобто, якщо відвернений збиток перевищує (дорівнює) економічні витрати на формування інформаційної безпеки підприємства, система інформаційної безпеки є ефективною.

Порівняльну економічну ефективність системи інформаційної безпеки підприємства пропонуємо визначати за перевищенням індексу економічного результату над індексом економічних витрат за формулою:

$$E_{і.п.} = \frac{\Delta З_2}{\Delta З_1} \div \frac{В_{і2}}{В_{і1}} > 1, \qquad (9.18)$$

де $Е_{і.\,п.}$ – показник порівняльної економічної ефективності поліпшення інформаційної безпеки підприємства, відносні од.;

$\Delta З_1$, $\Delta З_2$ – відвернений збиток, одержаний за рахунок системи інформаційної безпеки підприємства в базисному і новому періодах, грн/рік;

$В_{і1}$, $В_{і2}$ – економічні витрати на формування інформаційної безпеки підприємства у базисному і новому періодах, грн/рік.

У цьому випадку розглянуто для порівняння два періоди. Але порівнюватися можуть планові й фактичні результати та витрати. Якщо треба вибрати кращий варіант інформаційної безпеки з декількох варіантів (більше ніж двох), критерієм вибору слугує максимальне значення показника абсолютної економічної ефективності, який розраховується за кожним варіантом ($Еі = max$).

Відповідно до економічної теорії економічні витрати на створення інформаційної безпеки підприємства можна розраховувати як суму бухгалтерських витрат та умовного прибутку за формулою:

$$B_i = B_{б.\,i.} + E_н \times B_{б.\,i.}, \quad (9.19)$$

де B_i ($B_{б.\,i.}$) – економічні (бухгалтерські) витрати на створення системи інформаційної безпеки підприємства, грн/рік;
$E_н$ – нормативний показник економічної ефективності, відносні од.

Нормативний показник розраховується на рівні нормативного значення рентабельності продукції. Він дорівнює відношенню нормативного прибутку підприємства до собівартості реалізованої продукції.

Показник порівняльної економічної ефективності дає можливість розрахувати річний економічний ефект (ΔW_i), який буде одержано за рахунок упровадження кращого варіанта системи інформаційної безпеки підприємства:

$$\Delta W_i = (\Delta З_2 - \Delta З_1) \times \frac{B_{i1}}{\Delta З_2} - (B_{i2} - B_{i1}). \quad (9.20)$$

Виникає запитання: чи можна розрахувати вплив аудиту інформаційної безпеки, який є основною складовою її забезпечення, на економічну ефективність створення служби інформаційної безпеки. В економічній літературі не розглядалося питання щодо визначення впливу окремої складової. Пропонуємо такий вплив визначати за формулою:

$$K_i = \frac{\Delta W_{ai}}{\Delta W_i}, \quad (9.21)$$

де K_i – коефіцієнт, який визначає вплив аудиту захисту даних на економічну ефективність системи інформаційної безпеки підприємства, відносні од.;
ΔW_{ai} – річний економічний ефект, одержаний за рахунок проведення аудиту інформаційної безпеки підприємства, грн/рік;
ΔW_i – річний економічний ефект, одержаний за рахунок поліпшення системи інформаційної безпеки підприємства, грн/рік.

Отже, наприкінці дослідження нами запропоновано: метод розрахунку абсолютної та порівняльної економічної ефективності

DOI https://doi.org/10.36059/978-966-397-319-7-9

внутрішнього аудиту інформаційної безпеки та метод визначення економічного ефекту від впровадження аудиту захисту даних. Методи оцінювання ефективності аудиту інформаційної безпеки дадуть змогу підприємству визначити необхідність проведення внутрішнього аудиту та приймати обґрунтовані і доцільні рішення стосовно захисту даних.

Методи визначення абсолютної й порівняльної економічної ефективності впровадження системи інформаційної безпеки підприємства відрізняються від існуючих урахуванням перевищення відверненого збитку над економічними витратами. Це дає можливість економічно обґрунтувати створення системи інформаційної безпеки підприємства та її поліпшення. Метод визначення впливу аудиту захисту даних на економічну ефективність поліпшення інформаційної безпеки підприємства враховує частку економічного ефекту від проведення його аудиту в загальному ефекті впливу на підприємство.

ВИСНОВКИ

1. Рейдерством є силове недружнє поглинання підприємства проти волі його власника, що має переважне становище на даному підприємстві, або керівника; процес, пов'язаний з рейдерством, називається «рейдерське захоплення». У разі, якщо зловмисники мають намір поглинання підприємства, у власника є час та можливості для своєчасного виявлення підготовлюваного заходу за характерними ознаками, а саме: позови міноритарних акціонерів до суду, зображення підприємства у СМІ з поганого боку, часті перевірки з боку державних органів, поява мітингувальників під стінами підприємства тощо.

В Україні сьогодні рейдерське захоплення ІТ-бізнесу є досить нищівним чинником, що впливає на безпеку як ІТ-підприємств, так і країни зокрема. Для мінімізації та уникнення рейдерських дій в ІТ-сфері пропонуємо наступне: комп'ютерам, які використовуються для написання програм на замовлення, не надавати

можливість виходу до Інтернету; мати команду досвідчених юристів (бажано – з досвідом боротьби з рейдерством); прийняти законодавчі акти, які б не дозволяли рейдерам вдаватися до подібних заходів. Окрім того, з огляду на сучасні реалії, в яких опинилася наша держава це питання потребує постійного вивчення і напрацювання дієвих заходів з його уникнення.

2. Створення єдиної інформаційної системи для підприємства у вигляді desktop-застосунку – це найбільш ефективне рішення у сучасних умовах. Воно надає можливість більш раціонально використовувати фінансові ресурси у довгостроковій перспективі.

Диджиталізація здатна значно підвищити не лише ефективність окремих відділів, а і всього підприємства загалом. Проте, цільове використання різних програмних застосунків для підрозділів фірми не дадуть змогу повноцінно оцінити всі переваги від сучасних цифрових рішень. Саме через це значно ефективнішою буде використання єдиної інформаційної системи для керування підприємством.

Виявлено, що досліджені фактори дозволяють нівелювати ризики рейдерського захоплення підприємства. Їх використання значно ускладнює підготовку та збирання інформації зловмисниками, яку можна використати для подальшого нападу.

3. Врятуватися від рейдерського захоплення можна завдяки співпраці з досвідченими юристами та піарниками, які дадуть підприємцю можливість втримати контроль над власністю. Завдяки вказаним діям власник має змогу зберегти власне підприємство та захистити його від підготовлюваного нападу.

Жоден підприємець не застрахований від рейдерського нападу доти, доки на державному рівні не будуть прийняті заходи для унеможливлення рейдерства. Якщо заходи, які зазначено у роботі, будуть введені у дію, то проведення рейдерських захоплень буде надто складним, а, отже, невигідним.

4. Метою аудиту інформаційної безпеки є висловлення незалежної думки експерта-аудитора про стан надійності збереження та доступу до даних, достовірність, законність, правильність, точність дотримання інформаційної гігієни співробітниками підприємства, а також розробка пропозицій щодо попередження

DOI https://doi.org/10.36059/978-966-397-319-7-9

можливих загроз цілісності масиву документів та оптимізації витрат на забезпечення та підвищення рівня захисту інформації.

Весь функціонал інформаційної безпеки підприємства взаємопов'язаний між собою та однаково важливий для забезпечення збереження даних.

Від дотримання принципів аудиту інформаційної безпеки залежить надійність використовуваної та захищеність зберігаємої інформації. Вищенаведені принципи будуть використані для оцінювання ефективності проведення аудиту інформаційної безпеки підприємства.

Переваги проведення аудиту інформаційної безпеки підприємства, а саме: отримання реальної оцінки стану захищеності інформації підприємства; забезпечення керівництва інформацією про придатність комп'ютерного обладнання; впевненість у надійності системи інформаційної безпеки на підприємстві; здійснити діагностику ефективності роботи служби інформаційної безпеки підприємства; підтримування актуальної версії резервної копії на захищеному просторі підприємства; забезпечення безперебійної роботи системи пошуку та видалення вірусів; впровадження обов'язкових вимог до змісту паролів та своєчасне їх оновлення; унеможливлення збоїв або виходу із ладу комп'ютерного обладнання у випадку перевантаження системи підприємства; проведення інвентаризації наявного обладнання та встановленого ПЗ; проведення оновлення ПЗ та модернізації комп'ютерного обладнання; проведення аналізу існуючих загроз через наявність недоліків у системі інформаційної безпеки; надання рекомендацій щодо покращення антивірусного захисту даних на підприємстві.

Удосконалено аудит інформаційної безпеки підприємства, що на відміну від існуючих включає: анкету, загальний план аудиту, програму аудиту, робочі документи аудитора. Запропонована методика проведення перевірки надасть змогу аудитору охопити всі аспекти перевірки інформаційної безпеки підприємства, дослідити правильність, своєчасність, законність їх відображення, вчасно виявити порушення, провести якісний аудит, попередити загрози та оптимізувати витрати підприємства.

5. Проаналізували господарську діяльність на ТОВ «Запорізький ливарно-механічний завод». З'ясували, які функції виконує підприємство та як підтримує свою роботу під час воєнного стану.

Проаналізували витрати та прибуток ТОВ «Запорізький ливарно-механічний завод», де дізналися про додаткові витрати підприємства на допомогу ЗСУ. Надали пропозиції щодо удосконалення господарської діяльності підприємства, а саме: залучення іноземних інвестицій; участь у міжнародних програмах та грантових проєктах; залучення адміністративних відділів підприємства в отриманні прибутку шляхом надання послуг; економія витрат адміністративними відділами підприємства; залучення до співпраці ливарного заводу SOBOWIDZ, м. Гданськ, Польща; залучення науковців до розробок сучасних матеріалів та технологій виробництва, які необхідні у воєнний період для подолання російської агресії в Україні; залучення науковців до розробок сучасних матеріалів та технологій виробництва, які необхідні у післявоєнний період для відновлення інфраструктури та розбудови України. Це надасть збільшення прибутку та підвищення ефективності діяльності підприємства.

Провівши дослідження, варто відмітити важливе положення промислових підприємств в Україні у цілому. При інтенсивних бойових діях, вони продовжують свою роботу навіть із такими проблемами, як: логістичні перебої, ракетні обстріли підприємств, брак коштів як на самому підприємстві, так і у державному бюджеті і все задля того – щоб якнайшвидше прискорити Перемогу українського народу в цій жахливій та затяжній війні.

Удосконалено аудит методів боротьби з загрозами інформаційної безпеки та ефективності господарської діяльності, що на відміну від існуючих включає: анкету, загальний план аудиту, програму аудиту, робочі документи аудитора. Запропонована методика проведення перевірки надасть змогу аудитору охопити всі аспекти перевірки методів боротьби з загрозами інформаційної безпеки, дослідити правильність, відповідність, законність їх відображення, вчасно виявити порушення, провести якісний аудит,

DOI https://doi.org/10.36059/978-966-397-319-7-9

попередити загрози, оптимізувати витрати та прибутки підприємства, а також підвисити ефективність діяльності.

За результатами проведеного дослідження нами запропоновано: метод розрахунку абсолютної та порівняльної економічної ефективності внутрішнього аудиту інформаційної безпеки та метод визначення економічного ефекту від впровадження аудиту захисту даних. Методи оцінювання ефективності аудиту інформаційної безпеки дадуть змогу підприємству визначити необхідність проведення внутрішнього аудиту та приймати обґрунтовані і доцільні рішення стосовно захисту даних.

Методи визначення абсолютної й порівняльної економічної ефективності впровадження системи інформаційної безпеки підприємства відрізняються від існуючих урахуванням перевищення відверненого збитку над економічними витратами. Це дає можливість економічно обґрунтувати створення системи інформаційної безпеки підприємства та її поліпшення. Метод визначення впливу аудиту захисту даних на економічну ефективність поліпшення інформаційної безпеки підприємства враховує частку економічного ефекту від проведення його аудиту в загальному ефекті впливу на підприємство.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Меліхов Є. В., Макаренко А. П. Безготівкові розрахунки – основа сучасної торгівлі. Підприємництво в аграрній сфері: глобальні виклики та ефективний менеджмент : матеріали І Міжнародної наук.-практ. конф. (12–13 лютого 2020 р.). У 2 ч. Запоріжжя : ЗНУ, 2020. Ч. 1. С. 515–516.
2. Меліхов Є. В., Макаренко А. П. Дистанційний зв'язок як сучасний інструментарій бізнесу. *Актуальні проблеми проведення економічних, товарознавчих, будівельних експертиз та правові шляхи їх вирішення* : матеріали Круглого столу. Запоріжжя : ЗНУ, 2020. С. 112–113.
3. Меліхов Є. В., Макаренко А. П. Захищеність від рейдерства банківської сфери. *Сучасні тенденції в розвитку банківської системи та фінансових ринків України* : матеріали XXIV Міжвузівської студентської наукової конференції. Дніпро : ДНУ, 2019. С. 42–44.

4. Меліхов Є. В., Макаренко А. П. Інформаційна безпека у еру інформаційних технологій. *Наукові та практичні підходи до проведення економічних, товарознавчих, будівельних експертиз* : матеріали Круглого столу. Запоріжжя : ЗНУ, 2019. С. 124–126.
5. Меліхов Є. В., Макаренко А. П. Проблемність споживання і заощадження у бюджеті населення. *Проблеми економічного розвитку у сучасних умовах* : зб. матеріалів доп. учасн. XXIII наук.-тех. конф. студентів, магістрантів, аспірантів і викладачів ЗДІА. Запоріжжя : ЗДІА, 2018. С. 227.
6. Меліхов Є. В., Макаренко А. П. Рейдерство як загроза економічної безпеки підприємства. *Сучасні проблеми та перспективи проведення економічних, товарознавчих, будівельних експертиз* : матеріали Круглого столу. Запоріжжя : ЗНУ, 2019. С. 91–93.
7. Меліхов Є. В., Макаренко А. П. Умови інтеграції банківської системи України у міжнародний фінансовий простір. *Сучасні тенденції в розвитку банківської системи та фінансових ринків України* : матеріали XXV Міжвузівської студентської наукової конференції. Дніпро : ДНУ, 2020. С. 286–288.
8. Меліхов Є. В., Макаренко А. П. Фундаментальна різниця між грошима і фінансами. *Економіка та менеджмент у період цифрової трансформації бізнесу, суспільства і держави* : матеріали Ювілейної Міжнародної науково-практичної конференції (м. Запоріжжя, 28–29 травня 2020 р.). Запоріжжя : ЗНУ, 2020. С. 180–181.
9. Меліхов Є. В., Міхайлуца О. М. Блокчеин как ключевой инструмент диджитализации общества. *Theory and practice: problems and prospects – 2020* : матеріали Міжнародної наук.-практ. конференції. Литва : Каунас, 2020. С. 61–63.
10. Меліхов Є. В., Міхайлуца О. М. Захищене програмування в основі будь-якого застосунку. *Комп'ютерні інтелектуальні системи та мережі* : матеріали XIII Всеукраїнської наук.-практ. WEB-конференції аспірантів, студентів та молодих вчених (24–26 березня 2020 р.). Кривий Ріг : КНУ, 2020. С. 236–238.
11. Меліхов Є. В., Міхайлуца О. М. Захищеність від рейдерства ІТ-сфери. *Молода наука – 2019* : збірник наукових праць студентів, аспірантів і молодих вчених. Запоріжжя : ЗНУ, 2019. Т. 5. С. 254–257.
12. Меліхов Є. В., Міхайлуца О. М. Перспективи диджиталізації цифрової освіти. *Вплив цифрової освіти на розвиток людського капіталу* : матеріали Міжнародної наук.-практ. інтернет-конференції (м. Запоріжжя, 20–21 листопада 2019 р.). Запоріжжя : ЗНУ, 2019. С. 184–186.
13. Меліхов Є. В., Міхайлуца О. М. Практичне застосування теорії графів. *Інформаційні технології в моделюванні* : матеріали

V Всеукраїнської наук.-практ. конференції студентів, аспірантів та молодих вчених (м. Одеса, 19–20 березня 2020 р.). Одеса : ОНПУ, 2020. С. 118–120.

14. Меліхов Є. В., Міхайлуца О. М. Формування розуміння необхідності постійного самовдосконалення зі шкільної лави. *Актуальні проблеми неперервної освіти в інформаційному суспільстві* : збірник матеріалів конференції. Київ : Вид-во НПУ імені М. П. Драгоманова, 2020. С. 200–202.
15. Меліхов Є. В., Макаренко А. П. Забезпечення збереження інформації як основа безпеки сучасного підприємства. *Круглий стіл на тему: «Дискусійні питання з теорії та практики сучасної експертизи»* : матеріали Круглого столу (м. Запоріжжя, 24 листопада 2020 р.). Запоріжжя : ЗНУ, 2020. С. 91–93.
16. Меліхов Є. В., Міхайлуца О. М. Технологія доповненої реальності в основі програмних застосунків майбутнього. *Формування концепції цифровізації як чинник розвитку креативності особистості та її вплив на розвиток людського й соціального капіталу* : матеріали Міжнародної науково-практичної конференції (м. Запоріжжя, 26–27 листопада 2020 р.). Запоріжжя : ЗНУ, 2020. С. 167–170.
17. Меліхов Є. В., Міхайлуца О. М. Створення єдиної інформаційної системи підприємства як основа диджиталізації України. *Економіка, фінанси, облік та право: стратегічні пріоритети розвитку в умовах глобалізації* : матеріали Міжнарод. наук.-практ. конф., 20 бер. 2023 р. Умань : ЦФЕНД, 2023. С. 46–47.
18. Меліхов Є. В., Міхайлуца О. М. Переваги впровадження єдиної інформаційної системи для керування підприємством в межах території України. *Молода наука – 2023* : збірник наукових праць студентів, аспірантів, докторантів і молодих вчених. 17–22 квітня 2023 р. Запоріжжя : ЗНУ, 2023. Т. 5. С. 104–106.
19. Меліхова Т. О. Економічна безпека промислових підприємств: аналіз фінансового стану, ймовірності банкрутства, чистого економічного ефекту від залучення інвестицій. *Теоретичні і практичні аспекти економіки та інтелектуальної власності* : зб. наук. праць. Маріуполь, 2018. Вип. 35. С. 215–222.
20. Меліхова Т. О., Салига С. Я. Формування фінансової безпеки суб'єктів господарювання на основі аудиту податків : монографія. Запоріжжя, 2011. 272 с.
21. Варналій З. С., Живко З. Б. Роль державних інституцій в удосконаленні державного регулювання у сфері протидії рейдерству. *Вісник Київського національного університету ім. Тараса Шевченка*. 2014. № 154. С. 12.

22. Гарагонич О. В. Етапи рейдерського захоплення акціонерних товариств. *Вісник Академії адвокатури України*. 2013. № 3 (28). С. 27–28.
23. Друзін Р. В. Засади забезпечення протидії недружньому злиттю і поглинанню підприємств. *Фінанси, банки, інвестиції*. 2013. № 5. С. 36.
24. Єфименко А. Рейдерство або ринок контролю. *Юридичний журнал*. 2008. № 11. С. 116–122.
25. Нестеренко В. Ю. Рейдерство в Україні: оцінка сучасного стану, причини та перспективи розвитку. *Проблеми і перспективи розвитку підприємництва*. 2011. № 1. С. 20–23.
26. Оксак А. Особливості ринку злиття та поглинання в Україні. *Теоретичні та прикладні питання економіки*. 2014. № 1 (28). С. 454–462.
27. Хакери опублікували дані клієнтів і, ймовірно, працівників великої української IT-компанії. *Новини України* : вебсайт. URL: https://nv.ua/ukr/biz/tech/ataka-na-softserve-hakeri-opublikuvali-dani-kliyentiv-ipracivnikiv-kompaniji-novini-ukrajini-50n2503.html (дата звернення: 09.04.2023).
28. Що таке рейдерство в аграрному бізнесі та як з ним боротися. *Юридична газета online*. URL: https://yur-gazeta.com/publications/practice/zemelne-agrarne-pravo/shcho-take-reyderstvo-v-agrarnomubiznesi-ta-yak-z-nim-borotisya.html (дата звернення: 12.04.2023).
29. Як грамотно захиститися від рейдерства: найпоширеніші помилки бізнесу. *Економічна правда*. URL: https://www.epravda.com.ua/projects/antyreid/2020/12/22/669323 (дата звернення: 12.04.2023).
30. Юрченко О. М. Рейдерство в Україні. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2 (28). С. 81–82.
31. 7 заходів для захисту сервера. *Hab*r : вебсайт. URL: https://habr.com/ru/company/galtsystems/blog/314344 (дата звернення: 09.04.2023).
32. Canon confirms ransomware attack in internal memo. *Bleepingcomputer* : вебсайт. URL: https://www.bleepingcomputer.com/news/security/canon-confirms-ransomware-attack-in-internal-memo (дата звернення: 09.04.2023).

DOI https://doi.org/10.36059/978-966-397-319-7-9