

Рекомендовано до видання, розміщення в електронній бібліотеці та використання в освітньому процесі вченою радою Вищого навчального закладу Укоопспілки «Полтавський університет економіки і торгівлі» (протокол № 6 від 19 травня 2021 р.).

Колектив авторів

Рецензенти:

К. А. Пилипенко, д. е. н., професор, професор кафедри бухгалтерського обліку та економічного контролю Полтавської державної аграрної академії;

Н. М. Малуга, д. е. н., професор, професор кафедри бухгалтерського обліку, оподаткування та аудиту Поліського національного університету.

Перспективи розвитку бухгалтерського обліку, аналізу та аудиту в умовах інноваційних інформаційних технологій : монографія / Є. А. Карпенко, О. В. Карпенко, А. І. Мілька [та ін.]. – Полтава : ПУЕТ, 2021. 410 с. – 1 електрон. опт. диск (CD-ROM).

ISBN 978-966-184-408-6

У монографії досліджуються проблеми й перспективи розвитку бухгалтерського обліку, аналізу та аудиту в умовах інноваційних інформаційних технологій. Приділено увагу виявленню чинників і передумов розвитку інформаційних технологій та напрямів трансформації організації бухгалтерського обліку, контролю й аналізу під впливом діджиталізації економіки.

Для фахівців у галузі бухгалтерського обліку, аналізу та аудиту, викладачів, співробітників, аспірантів і студентів економічних спеціальностей закладів вищої освіти.

УДК 657:657.62-043.86]:004.9

п. 4.7 – Хаджинова О. В., д. е. н., проф., декан, Державний вищий навчальний заклад «Приазовський державний технічний університет», Куртяник М. С., аспірант, Державний вищий навчальний заклад «Приазовський державний технічний університет»;

п. 4.8 – Костякова А. А., к. е. н., доц., доцент, Таврійський державний агротехнологічний університет імені Дмитра Моторного;

п. 4.9 – Кравченко О. В., к. е. н., доц., старший викладач, Сумський державний університет, Овчарова Н. В., студент, Сумський державний університет;

п. 4.10 – Демиденко Світлана Леонтіївна, к. е. н., доц., доцент, Черкаський державний технологічний університет;

п. 4.11 – Дутченко Олена Олегівна, к. е. н., доц., старший викладач, Сумський державний університет, Медвідь Жанна Василівна, спеціаліст з міжнародної фінансової звітності, ТОВ «НЕТКРЕКЕР»;

п. 4.12 – Калінін О. В., д. е. н., проф., ДВНЗ «Приазовський державний технічний університет», Богачов О., аспірант кафедри «Маркетинг та бізнес – адміністрування» ДВНЗ «Приазовський державний технічний університет»;

п. 4.13 – Максимова Ю. О., Одеський національний університет імені І. І. Мечникова;

п. 4.14 – Юрченко О. В., асистент, Центральноукраїнський національний технічний університет;

п. 4.15 – Артем'єва Оксана Олександрівна, к. е. н., доцент, Університет Державної фіскальної служби України.

Публікація містить результати досліджень, проведених в процесі виконання науково-дослідної теми «Перспективи розвитку бухгалтерського обліку, аналізу та аудиту в умовах інноваційних інформаційних технологій» (номер державної реєстрації 0115U002543)

розрахунки до кошторису, зведення показників спеціального фонду та інші).

Програмний продукт повинен надавати можливість експорту інформації про установу на веб-портал Є-Дата.

Впровадження програмного продукту може не тільки полегшити роботу бухгалтера, а й заощадити його робочий час, зменшити ризики помилок, а враховуючи наявність форс-мажорних обставин сьогодення (COVID-19), дозволить працювати дистанційно у віддаленому доступі. Завдяки цьому зникне потреба в здійсненні завдань в ручному режимі, таким чином можливо оптимізувати всю бухгалтерську роботу.

В Україні триває процес реформування бухгалтерського обліку та звітності в державному секторі відповідно до міжнародних стандартів бухгалтерського обліку. Метою цього процесу є наближення організації бухгалтерського обліку до сучасних вимог міжнародної практики, усунення можливих проблем, удосконалення нормативної бази, що регламентує облік [170].

Основними шляхами покращення організації обліку в установах бюджетної сфери є систематизація облікових процесів, покращення формування організаційної структури бухгалтерських служб, удосконалення системи підготовки та перепідготовки профільних спеціалістів. Все це можна забезпечити шляхом впровадження інформаційно-аналітичної системи суб'єктами державного сектору для ведення бухгалтерського обліку та складання фінансової звітності [170].

Організація бухгалтерського обліку в бюджетних установах регулюється вимогами чинного законодавства, зокрема: Бюджетного кодексу України та Податкового кодексу, Національними положеннями (стандартами) бухгалтерського обліку в державному секторі, Законом України «Про бухгалтерський облік та фінансову звітність в Україні та різними постановами і наказами Міністерства Фінансів та Кабінету Міністрів України.

Отже, за результатами проведеного дослідження можна дійти висновку, що ведення бухгалтерського обліку в бюджетних установах є досить складним та серйозним процесом, це потребує точності і достовірності.

4.12. Діджитал аналітика безпеки підприємницької діяльності сучасних підприємств

Калінін О. В., Богачов О.

Інциденти цифрової безпеки завдають шкоди бізнесу, урядам та приватним особам, підриваючи доступність, цілісність та конфіденційність їх даних, інформаційних систем та мереж. Підприємницькі структури зазнають матеріальних та нематеріальних збитків, включаючи грошові втрати, зни-

ження конкурентоспроможності, збиток репутації, переривання операцій та порушення конфіденційності. З появою споживчого та промислового Інтернету речей, що поєднує мережу Інтернету, збитки можуть поширитися на фізичне середовище та вплинути на безпеку.

Виникає необхідність дослідження тенденції щодо ризиків цифрової безпеки та політики цифрової безпеки. Основна увага приділяється політиці, яка заохочує інновації цифрової безпеки, покращує цифрову безпеку продуктів та покращує управління вразливістю. Також це відкриває нові можливості, що виникають завдяки штучному інтелекту (ШІ) для цифрової безпеки.

Ризик цифрової безпеки виникає внаслідок інцидентів, спричинених загрозами, що використовують вразливі місця. До джерел загроз належать уряди, групи та особи зі зловмисними або злочинними цілями. Їх мотивація різниться, але, як правило, включає геополітичні цілі урядів. Інциденти також можуть виникати внаслідок ненавмисних загроз, таких як людська помилка або відключення електроенергії.

Аналіз видів безпеки, пов'язаних цифровими технологіями в світі дозволив виявити найбільш поширені:

1. Атаки розподіленої відмови в обслуговуванні (DDoS) – це поширений тип інциденту, який порушує роботу інтернет-служби, заливаючи її нелегітимними запитами. Дані про DDoS-атаки, як правило, надходять від компаній, що пропонують послуги пом'якшення DDoS. Вони не мають вичерпної картини ландшафту, але можуть надати корисну інформацію про ключові тенденції.

2. Фішинг залишається високим і виявляється важчим для людини.

У фішингу, одному з головних векторів, зловмисники маскують себе як надійну особу в Інтернет-спілкуванні. Таким чином, вони отримують конфіденційну інформацію, таку як імена користувачів та паролі, або доставляють шкідливий код («шкідливе програмне забезпечення»). Існують різні типи фішингових атак. Повідомлення про фішинг часто містять посилення на шкідливі веб-сайти, які кінцевим користувачам дедалі важче виявити без використання автоматизованого захисту. Широкі нецільові кампанії мають на меті збирати дані, направляючи користувачів на підробку електронної комерції або фінансових веб-сайтів. Більш складні електронні листи спрямовані на конкретних людей, щоб вони заклали шкідливе програмне забезпечення в інформаційну систему їх організації (спеар-фішинг).

У країнах Європейського Союзу фішинг та фармінг (які переспрамовуються на фальшиві веб-сайти, що вимагають особисту інформацію) сильно відрізняються в різних країнах (рис. 4.20).

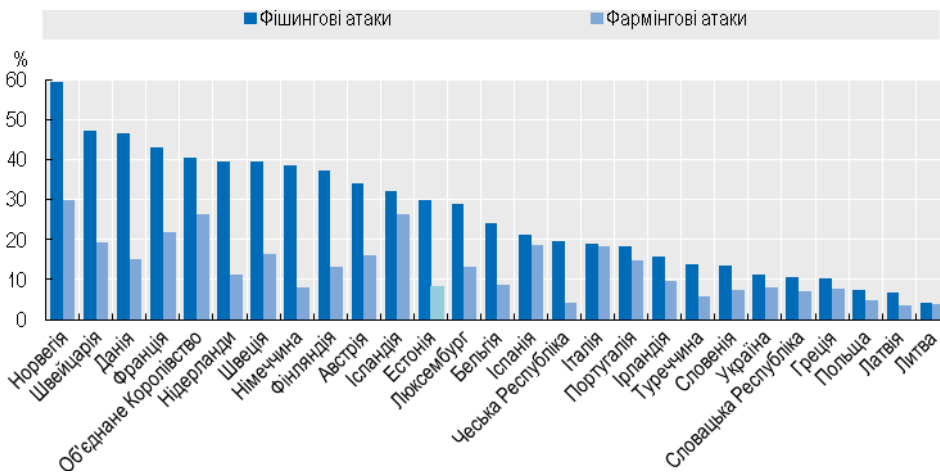


Рисунок 4.20 – Особи, які зазнали фішингових та фармінгових атак, 2019 відсотках від усіх користувачів Інтернету

Примітки. Фішинг стосується отримання шахрайських повідомлень. Фармінг стосується перенаправлення на фальшиві веб-сайти з проханням надати особисту інформацію.

Різні фактори можуть сприяти поясненню цих відмінностей. Сюди входять недостатня обізнаність / розуміння спроб фішингу та / або неможливість їх ідентифікувати, національні мови, заходи безпеки, пропоновані постачальниками послуг електронної пошти та Інтернету (ISP) тощо. За даними Symantec, підводний фішинг залишався найпопулярнішим напрямком цілеспрямованих атак у 2018 році. Його використовували 65 % усіх відомих кіберзлочинців та державних груп. За даними Verizon, 32 % порушень даних у 2018 році стосувалися фішингової діяльності. Фішинг був присутній у 78 % випадків шпигунства цифрової безпеки, включаючи встановлення та використання бекдорів.

3. Вимірjувальне програмне забезпечення – це тип шкідливого програмного забезпечення, яке використовує криптографію для обмеження або відключення доступності даних і вимагає викуп для відновлення. Вимагальні програми – це форма цифрового вимагання. Незважаючи на те, що вимога програм існує вже багато років, вона потрапила в загальні новини в 2017 році.

Ці гучні атаки допомогли підвищити обізнаність про цифрову безпеку та заохотили багато підприємств та організацій посилити свої основні заходи безпеки, включаючи плани резервного копіювання та відновлення.

Вимагач може паралізувати фізичні операції на заводах та у виробничих середовищах. Якщо зловмисники отримують доступ до системи інформаційних технологій (ІТ), вони можуть успішно спрямувати свою атаку на інфраструктуру операційних технологій (ОТ), яка управляє фізичними установками.

4. Криптовалюти. Протягом останніх п'яти років застосовували різні засоби, щоб використати зростаючий інтерес до криптовалют.

Найчастіше криптовалюти крадуть з бірж криптовалют. У період з 2012 по 2019 рік щонайменше 42 успішні атаки потрапляють на біржі. Наприклад, у 2019 році 12 атак призвели до крадіжки криптовалют на 292 мільйони доларів США. У 2018 році вісім атак призвели до крадіжки 844 млн дол. США Деякі з цих атак призвели постраждалі компанії до банкрутства.

Протягом останніх трьох років розроблено більш непомітні техніки, які називаються криптовалютою та криптоджекінгом. Криптовалюта відбувається, коли злочинці встановлюють шкідливе програмне забезпечення, яке узурпує обробну потужність користувача для видобутку криптовалют. Криптоджекінг – це криптовалюта за допомогою скриптів, вставлених у веб-вміст, що працює в браузері користувача.

5. Шкідливе програмне забезпечення стає все більш досконалим

Безфайлове шкідливе програмне забезпечення менш видиме, оскільки код виконується лише в пам'яті системи або використовує зазвичай дозволені інструменти, встановлені в системі. Шкідливе програмне забезпечення перетворилося із зашифрованого на олігоморфне до поліморфного та метаморфічного. Зашифроване зловмисне програмне забезпечення – це перший крок до уникнення виявлення на основі підписів. При кожному зараженні шкідливе програмне забезпечення шифрується за допомогою іншого ключа, що робить кожен файл унікальним. Однак засоби захисту все ще можуть виявити дешифрувач, що входить до коду, який його розшифровує, і залишається незмінним серед заражень.

Олігоморфне шкідливе програмне забезпечення може змінювати свій дешифрувач при кожному поколінні шкідливого коду, тобто кожного разу, коли код поширюється в інше місце. Але ця техніка може створити лише кілька сотень різних поколінь, чого недостатньо, щоб уникнути засобів безпеки.

Поліморфне шкідливе програмне забезпечення може створити незліченну кількість дешифрувачів за допомогою механізму мутації. Неможливо виявити за допомогою простих засобів захисту на основі підписів. Метаморфічні шкідливі програми можуть повністю переписати свій код. Таким чином, кожна нова версія, що поширюється в інших місцях, більше не відповідає попередній ітерації без використання шифрування. Таким чином, виникає потреба щодо розробки заходів з управління цифровими ризиками в бізнесі.

З огляду на складність управління цифровими ризиками безпеки, складно визначити кількісно, наскільки підприємства впроваджують передові практики в цій галузі. Тим не менше, кілька останніх статистичних показників дають корисну інформацію. Вони вимірюють конкретні аспекти, які можуть бути використані як довірені особи для формування відносно вагомого уявлення про цю ситуацію Україні. Вони стосуються підприємницьких структур, які оцінюють ризик цифрової безпеки, інформують своїх працівників про зобов'язання щодо цифрової безпеки, проводять тести безпеки або регулярні резервні копії та страхують від інцидентів цифрової безпеки. Оцінка ризиків цифрової безпеки – періодична оцінка ймовірності та наслідків інцидентів цифрової безпеки – є основою управління цифровими ризиками безпеки. Загалом частка підприємств, які проводять оцінку ризику, коливається від 14 % в Україні до 60 % у Фінляндії. Що стосується інших показників цифрової безпеки, то ця частка в середньому зростає із збільшенням розміру фірм. Це менше однієї третини серед малих фірм, але майже три чверті серед великих фірм (рис. 4.21).

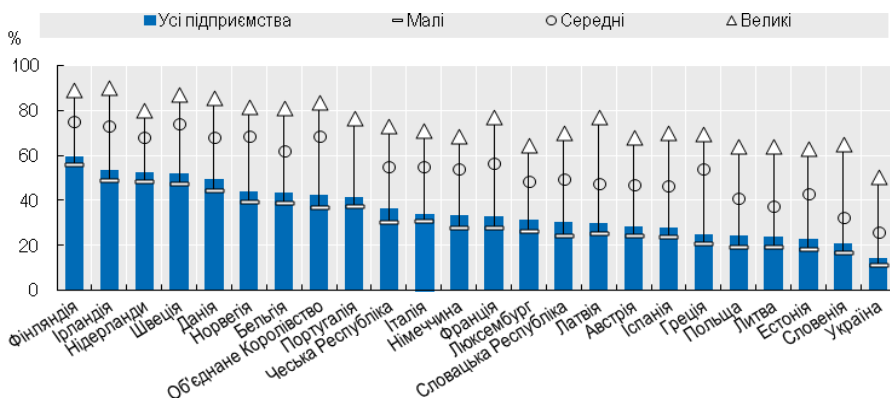


Рисунок 4.21 – Підприємства, які проводять оцінку ризиків ІКТ, за розміром, 2019

Джерело : ОЕСР на основі Євростату (2019 [372]), Цифрова статистика економіки та суспільства , Всесвітня база даних (доступ в березні 2020 року).

Цифрова оцінка ризику безпеки є надзвичайно важливою, щоб допомогти вирішити, що робити з ризиком. Ризик можна зменшити або перенести. Її також можна приймати або усувати, хоча усунення усуває як ризик, так і користь. Щоб знизити ризик до прийнятного рівня, фірми повинні обирати заходи безпеки, пропорційні ризику та контексту. Занадто велика безпека заважає економічній та соціальній діяльності, яку захищають заходи без-

пеки. Занадто мала безпека не призведе до достатнього зниження ризику. Заходи безпеки можуть включати тести безпеки, процедури резервного копіювання, методи криптографії, двофакторну автентифікацію, контроль доступу до мережі та використання віртуальних приватних мереж.

Аналіз довів, що практика оцінки ризиків суттєво корелює з тестами безпеки або процедурами резервного копіювання (рис. 4.22).

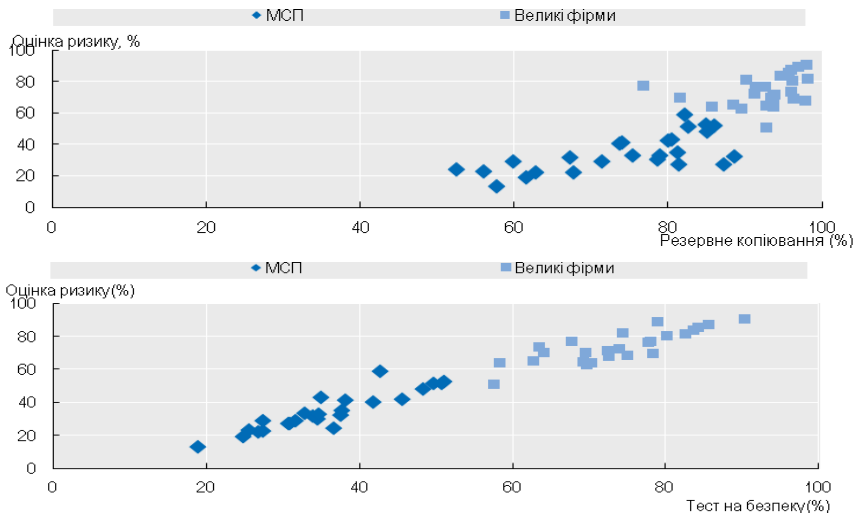


Рисунок 4.22 – Оцінка ризиків, тести безпеки ІКТ та резервне копіювання у малих та великих фірмах, 2019

Примітки: МСП = малі та середні підприємства. «Тести безпеки ІКТ» стосуються таких видів діяльності, як проведення тестів на проникнення, тестування систем оповіщення про безпеку, перегляд заходів безпеки або тестування резервних систем. «Резервне копіювання» означає резервне копіювання даних в окреме місце (включаючи резервне копіювання в хмару).

Як спостерігається для інших показників безпеки ІКТ у цьому розділі, великі підприємницькі структури здійснюють цю діяльність в середньому набагато частіше, ніж малі. Крім того, мінливість у різних країнах порівняно схожа між великими та малими структурами для тестування на безпеку. Це свідчить про те, що резервне копіювання у великих підприємствах є частиною основних практик цифрової безпеки, тоді як у МСП воно більш чутливе до практики оцінки ризиків. Одним із засобів зниження ризику є прийняття рішення про передачу ризику, придбавши страховку. Схильність підприємницьких структур до придбання страхового полісу дуже варіюється – вона становить від 4 % у Литві до понад 56 % у Данії. У всіх країнах ЄС, крім

двох, схильність зростає із збільшенням розміру підприємств. У Данії він значно вищий серед малих підприємств (57 %) порівняно із середніми (5 %) та великими (40 %). Це також має місце у Словенії, хоча в значно меншій мірі (рис. 4.23).

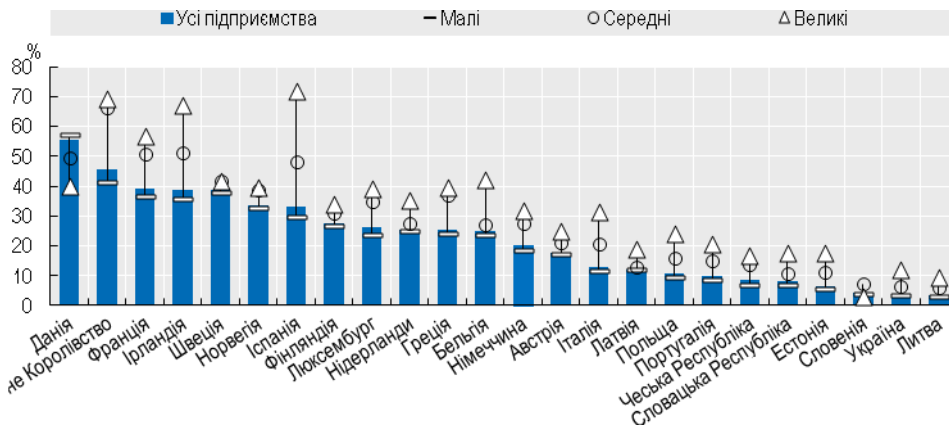


Рисунок 4.23 – Підприємства, що мають страхування від випадків безпеки ІКТ за розміром, 2019

Загалом, схильність до придбання страхування можна розглядати як ознаку того, наскільки серйозно фірми ставляться до цифрової безпеки. Однак це також залежить від того, наскільки в країні доступні страхові поліси, що покривають ризик цифрової безпеки. Ринок цифрового страхування безпеки є складним. Традиційні страхові поліси або самостійні поліси «кіберстрахування» можуть покривати ризики. Як результат, деякі компанії можуть думати, що традиційна політика охоплює їх, коли вони цього не роблять.

Ще одним показником прихильності до цифрової безпеки є частка підприємств, які інформують людей, які працюють, про свої зобов'язання з питань, пов'язаних з безпекою ІКТ. Він коливається від однієї третини в Греції до більш ніж трьох чвертей в Ірландії, де також спостерігається велика концентрація бізнесу в секторі ІКТ, часто багатонаціональних плацдармів для Європи. Ця частка також зростає із збільшенням розміру підприємств: менше 60 % серед малих підприємств, але більше 90 % серед великих підприємств (рис. 4.24).

У більш загальному плані всі вищезазначені показники, засновані на даних Євростату, чітко свідчать про схильність фірм до запровадження заходів цифрової безпеки, що зростають із збільшенням їх розміру. Крім того, ця схильність також систематично вища для фірм у певних галузях, таких як сектор ІКТ, або професійної, наукової та технічної діяльності. Крім того, оцінка ризику також вища, в середньому, у сфері нерухомості.

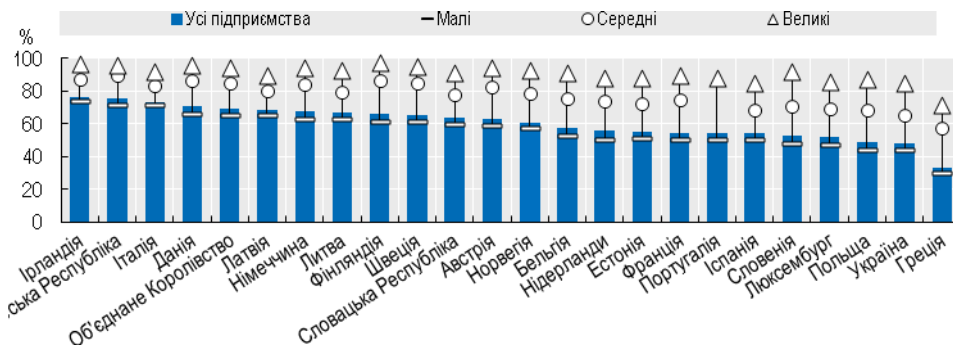


Рисунок 4.24 – Підприємства, які інформують працевлаштованих осіб про свої зобов’язання з питань, пов’язаних із безпекою ІКТ, за розміром, 2019

Доведено, існують перешкоди для широкого прийняття системи цифрової безпеки. Багато політиків ще недостатньо усвідомлюють необхідність усунення таких перешкод та заохочують відповідальну поведінку всіх зацікавлених сторін.

Проведений аналіз дозволив розробити рекомендації з цифрової безпеки діяльності. Вони спрямовані на те, щоб діяльність зосереджувалась на тому, що є критично важливим для економіки та суспільства, не накладаючи непотрібних обтяжень для решти. Основними напрямками є:

адаптація їх всеохоплюючої політики;

забезпечення того, щоб оператори ефективно знижували ризик цифрової безпеки до критичних функцій до рівня, прийняттого для суспільства;

сприяння та побудова партнерських відносин на основі довіри;

покращення співпраці на міжнародному рівні.

Рекомендація також роз’яснює, як ця сфера співвідноситься із ширшою національною політикою управління ризиками.

Цей процес повинен відбуватися на основі національної оцінки ризику, що охоплює всю економічну та соціальну діяльність:

Уряд, працюючи з відповідними державними та приватними суб’єктами, визначає:

1. Критичні види діяльності, пов’язані з цифровою безпекою.
2. Операторів цих важливих видів діяльності; на підприємствах:
3. Здійснюється циклічне управління ризиками для виявлення функцій, без яких вони не могли б ефективно виконувати свою;
4. Складається карта «цифрової екосистеми», тобто цифрового середовища, яке підтримує їх функції по ланцюжку створення вартості результатів діяльності;

5. Проводиться циклічна оцінку ризиків цифрової безпеки критичних функцій, беручи до уваги їх цифрову екосистему, та визначається на цій основі рівень ризику цифрової безпеки, який слід зменшити, перенести, уникнути та прийняти («лікування ризиків») та заходи з управління цифровою безпекою а також ті, що захищають діяльність, виявляють інциденти та реагують на них та встановлюють стійкість.

Перші три етапи цього процесу, є частиною більш широкої національної системи управління ризиками та політики захисту критичної інфраструктури, та зосереджуються на цифровій безпеці. Зазначити їх важливо для забезпечення узгодження етапів четвертого та п'ятого з національною оцінкою ризику та не створювати зайвого навантаження для операторів.

Вважаючи діяльність відповідно до наданих рекомендацій, це створить додаткові обмеження для операторів та може вплинути на їх конкурентоспроможність на світовому ринку. Тому уряди часто співпрацюють з цими операторами та іншими зацікавленими сторонами на першому та другому етапах, і, загальніше, у процесі формування політики, щоб найкращим чином збалансувати прогрес у цифровій безпеці з економічними та соціальними показниками.

Крок четвертий вводить поняття «цифрова екосистема», яке є ширшим, ніж інформаційні системи та мережі, включає цифрові активи, такі як апаратне забезпечення, програмне забезпечення, мережі та дані, операційні технології, що виявляють або викликають зміни у фізичних процесах, а також внутрішні та зовнішні сутності, особи та процеси, які проектують, підтримують та експлуатують їх, та взаємозв'язки між ними. Крок четвертий – це обов'язкова умова п'ятого кроку, коли оператори управляють ризиком цифрової безпеки, тобто як частина їх ширшої системи управління ризиками підприємств та загальних процесів прийняття економічних та соціальних рішень.

Враховуючи роль оцифровки в стимулюванні розвитку нових джерел сталого зростання, інновацій, зайнятості, добробуту та інклюзивності; і до відповідної ролі, з метою максимізації економічних та соціальних вигод цифрової економіки виникає необхідність посилення механізмів, що дозволяють брати участь всім зацікавленим сторонам у процесах розробки політики, включаючи уряди, міжнародні організації, бізнес, громадянське суспільство, організовану працю, технічну спільноту Інтернету та наукові кола.

Доведено, що сила та динамічність цифрової економіки залежать від ефективного доступу користувачів та новаторів до комунікаційної інфраструктури та послуг через високошвидкісні мережі, від більш ефективного використання цифрових технологій бізнесом, урядами, приватними особами та суспільством, від відкритості та від довіра користувачів;

Подальше визнання того, що вироблення політики, пов'язане з цифровою трансформацією, вимагає інтегрованого державного підходу та співпраці з усіма відповідними зацікавленими сторонами.

Цифрова залежність від критично важливих видів діяльності зростає і в даний час прискорюється завдяки цифровій трансформації та узагальненню таких технологій, як великі дані, штучний інтелект та Інтернет речей. Паралельно цифрові загрози безпеці зростають у кількості та вдосконаленні. Багато урядів очікують, що в найближчі роки інциденти з цифровою безпекою, що зачіпають критично важливі дії, можуть призвести до масштабних катастроф.

За результатами дослідження запропоновано заходи, які спрямовано на вирішення питань цифрової безпеки підприємницької діяльності. Їх впровадження забезпечує надійну основу для посилення цифрової безпеки економічної та соціальної діяльності без зменшення можливостей, що надаються цифровою трансформацією.

Запровадження даних заходів в практичній діяльності сприятиме посиленню цифрової безпеки окремих підприємств, не накладаючи непотрібного тягаря на інших суб'єктів.

Як вже було доведено:

- Цифрова трансформація впливає на всю економічну та соціальну діяльність, стимулюючи інновації та приносячи значні вигоди, але також піддає цю діяльність зростанню ризику цифрової безпеки;

- Ризик цифрової безпеки виникає внаслідок потенційних навмисних або ненавмисних загроз, які мають транскордонний характер, експлуатують вразливі місця та спричиняють інциденти, що впливають на доступність, цілісність та конфіденційність даних, обладнання, програмного забезпечення та мереж, на які покладається ця діяльність;

- Визначаючи, що множинність та складність цифрових залежностей між секторами, а також уздовж ланцюжків створення вартості видів діяльності створюють спільний цифровий ризик безпеки, який жоден учасник виробничого процесу не може суттєво зменшити для всіх.

- Партнерські відносини в державному та приватному секторах та між ними мають є важливе значення для узгодженого та цілісного підходу до ризику цифрової безпеки.

- Заходи, що проводяться різними операторами в різних секторах та країнах, залежать від одних і тих самих цифрових технологій, і тому можуть бути одночасно порушені загрозами, що використовують загальну вразливість; що інциденти цифрової безпеки можуть надзвичайно швидко поширюватися між операторами, секторами та кордонами; і що перебої у проведенні критично важливих заходів, спричинених інцидентами цифрової безпеки в одному місці, можуть переходити на інші оператори, сектори та країни, що потенційно може вплинути на регіони та міжнародну стабільність;

– наслідки інцидентів цифрової безпеки, можуть виходити за межі інтересів цих операторів, впливати на ціле суспільство та інших осіб за кордоном; і що, як наслідок, будь-який залишковий ризик, який приймають ці оператори, може вплинути на всіх, хто залежить від такої діяльності, а також на суспільство в цілому;

– підвищення цифрової безпеки видів діяльності є пріоритетом національної політики; що розбіжності в державній політиці в різних країнах збільшують складність управління цифровою безпекою взаємозалежних критичних видів діяльності за кордоном; і тому міжнародне співробітництво є вкрай важливим для зменшення таких розбіжностей та максимізації глобальної ефективності внутрішньої політики;

– управління ризиком цифрової безпеки повинно поважати конфіденційність та захист персональних даних;

Отже, цифрова екосистема означає цифрове середовище, яке підтримує підприємства по ланцюжку створення вартості критичних видів діяльності. Вона включає цифрові активи, такі як апаратне забезпечення, програмне забезпечення, мережі та дані, операційні технології, що виявляють або спричиняють зміни у фізичних процесах, а також внутрішні та зовнішні сутності, особи та процеси, що проектують, підтримують та експлуатують їх, та взаємозв'язки між ними.

Розробка стратегічного підходу до розробляють стратегічний підхід до управління цифровим ризиком безпеки повинно відбуватися шляхом:

1. Прийняття на вищому рівні національної стратегії цифрової безпеки, в якій зазначено чіткі цілі щодо посилення цифрової безпеки та стійкості до видів діяльності, а також забезпечення узгодженості з національною оцінкою ризиків та іншими стратегіями ризику та сектора.

2. Створення внутрішнього механізму управління, який розподіляє повноваження та відповідальність між конкретними структурами за розробку та реалізацію разом із відповідними зацікавленими сторонами політики з метою підвищення цифрової безпеки всередині та між секторами.

3. Забезпечення внутрішньої координації з метою:

налагодження співробітництва, беручи до уваги всю важливість діалогу між цифровою безпекою та галузевими експертами;

забезпечення узгодженості заходів;

ефективного розподілу ресурсів.

Підприємствам рекомендовано нарощувати спроможність підтримувати цифрове управління ризиками безпеки та стійкість шляхом:

1. Розробка нових або посилення існуючих можливостей реагування на інциденти, наприклад, через одну або більше груп реагування на надзвичайні ситуації комп'ютера (CERT), груп реагування на аварії комп'ютерної безпеки (CSIRT) та / або центрів безпеки (SOC), відповідальних за моніто-

ринг, попередження, попередження та проведення заходів з відновлення, а також механізмів для сприяння тіснішому співробітництву та комунікаціям серед тих, хто бере участь у реагуванні на інциденти.

2. Сприяння співпраці між CERT / CSIRT / SOC та операторами, включаючи звітування та аналіз інцидентів, для сприяння швидкому та ефективному оперативному співробітництву;

3. Застосування найкращої практики управління цифровими ризиками безпеки, пов'язаної з наданням урядом важливих цифрових заходів .

4. Просування міжнародних стандартів цифрової безпеки, методологій, базових посібників з безпеки, найкращих практик та інструментів;

5. Надання підтримки операторам шляхом обміну інформацією про загрози, вразливості та практику управління ризиками.

6. Сприяння розвитку світового ринку для різноманітних надійних служб безпеки та продуктів, включаючи керовані послуги, послуги з аудиту та реагування, включаючи, де це доречно, цілий ряд механізмів для достовірної сигналізації про природу та ступінь безпеки;

7. Підтримка розвитку кваліфікованої робочої сили, яка може управляти міжсекторними та галузевими ризиками цифрової безпеки;

8. Прийняття та заохочення прийняття відповідальних та скоординованих процесів розкриття та управління вразливими місцями, а також заохочення та захист дослідників безпеки.

9. Спільне використання, відповідно до операторів та інших суб'єктів, належним чином зведених статистичних даних із звітування про інциденти;

Під час реалізації механізму забезпечення цифрової безпеки запропоновано наступні методи роботи:

1) Зміцнити основи цифрової економіки шляхом розробки, моніторингу та просування послідовної політики та нормативної бази, яка зокрема:

а) стимулює конкуренцію та інвестиції у високошвидкісне ширококутне підключення та сприяє зближенню та сприяє повсюдному доступу до ширококутних мереж, послуг, програм та пристроїв;

б) сприяє інвестиціям у цифрові технології та капітал, заснований на знаннях, та покращує доступність та використання даних;

в) зменшує бар'єри для доступу до цифрових технологій та їх використання;

г) сприяє дослідженню, інноваціям та новим можливостям для бізнесу, включаючи ті, що виникають внаслідок нових технологій та додатків, одночасно розглядаючи їхні економічні та соціальні наслідки, та оцінюючи доцільність політичної та нормативної бази та глобальних стандартів;

д) Зміцнює довіру до цифрової економіки, в тому числі шляхом сприяння управлінню ризиками цифрової безпеки для економічної та соціальної діяльності та захисту конфіденційності, а також розробкою стратегій передачі

даних та міжнародних домовленостей, що сприяють сумісності між системами.

2) координувати роботу з іншими підприємницькими структурами з метою:

а) розробки аналізів, політики та передової практики, які використовують потенціал цифрової трансформації для зростання та добробуту за рахунок посилення підприємництва, навичок ІКТ та зайнятості та покращення стану здоров'я, добробуту та старіння;

б) подальшої розробки та впровадження середньо- та довгострокової дорожньої карти вимірювань для цифрової трансформації.

3) Інформувати про розробку політики щодо цифрової економіки, зокрема:

а) Перегляд та аналіз нових технологій;

б) аналіз економічних та соціальних наслідків розвитку та використання цифрових технологій в економіці; а також наслідків порушення цифрової безпеки та конфіденційності для економіки та суспільства;

в) Розробка засобів вимірювання та методології, включаючи використання Інтернету як джерела статистики, для зміцнення бази даних для цифрової економіки та оцінки її внеску в економіку в цілому;

г) приймати участь на рівні країни у співпраці з іншими відповідними комісіями з метою використання інноваційного досвіду та передової практики в окремих країнах, надання волонтерським країнам оцінки ступеня цифрової зрілості і допомоги політикам забезпечити злагоджений та згуртований підхід уряду, щоб краще реагувати на цифрову трансформацію та змусити її працювати на зростання та добробут.

4.13. Ефективність використання адаптивних систем документообігу на підприємствах

Максимова Ю. О.

Автоматизовані системи сьогодні все більше застосовуються в різноманітних сферах діяльності. Високу актуальність набуває можливість впровадження автоматизованих систем управління для малих і великих підприємств. Проблемами при побудові автоматизованих систем є відсутність можливості динамічно вносити зміни в систему, функції програмуються безпосередньо в коді, при необхідності внесення змін необхідно звертатися до відповідного ІТ фахівця. Розвиток таких систем призводить до підвищення вартості проектування автоматизованої системи на підприємстві.

Важливим етапом інформатизації суспільства є поступовий перехід від класичної паперової документації до електронних документів. Використання автоматизованих систем управління документацією має величезне зна-