УДК 339.9
DOI https://doi.org/10.32782/2524-0374/2023-8/74

КЛАСИФІКАЦІЯ ТА ОРГАНІЗАЦІЯ ЗАХИСТУ АКТИВІВ ПІДПРИЄМСТВА

CLASSIFICATION AND ORGANIZATION OF PROTECTION OF ENTERPRISE ASSETS

Шепета О.В., к.ю.н., доцент

У статті розглянуто класифікацію та оранізацію захисту активів підприємства. Вказано, що усі активи підприємства необхідно чітко ідентифікувати, скласти і підтримувати їх інвентарний опис. А також, що підприємство повинно всі активи задокументувати та окреслити їх важливість. Зазначено, що інвентарний опис активів підприємства повинно містити всю інформацію, необхідну для відновлення після лиха, в тому числі, тип активу, формат, розташування, резервну та ліцензійну інформацію та бізнес-цінність. Інвентарний опис не повинен дублювати інші описи, проте треба гарантувати узгодженість їх змісту. Значну увагу приділено важливості класифікації інформації для ідентифікації потреби, пріоритетності та очікуваного ступеня захисту під час її оброблення.

Автором зазначено, що інформація повинна бути класифікована в термінах її цінності, правових вимог, чутливості та критичності для підприємства. А також визначений рівень захисту інформації може бути оцінений шляхом аналізу конфіденційності, цілісності, доступності та будь-яких інших вимог до розглядуваної інформації.

Зазначено, що для кожного класифікаційного рівня повинні бути визначені процедури поводження з інформацією, охоплюючи безпечну обробку, зберігання, передавання, розкласифікацію (виведення з класифікації) та знищення. Вони повинні містити також процедури для ланцюга охорони та реєстрації будь-якої події, суттєвої для безпеки.

Визначено що угоди з іншими організаціями, які охоплюють спільне використання інформації, повинні містити процедури ідентифікації класифікації такої інформації та інтерпретації класифікаційних позначок інших організацій. Маркування та безпечне оброблення класифікованої інформації є ключовою вимогою угод щодо спільного використання інформації. Фізичні позначки є загальноприйнятою формою маркування. Проте, деякі інформаційні активи, такі як документи в електронному вигляді, не можуть бути фізично позначені і потребують використання електронних засобів маркування

Акцентовано увагу, що для всіх активів повинні бути ідентифіковані їх власники і повинна бути встановлена відповідальність за підтримування належних контролів.

Ключові слова: захист інформації, активи підприємства, класифікація інформації, класифікація активів підприємства.

The article deals with the classification and organization of the protection of the company's assets. It is indicated that all assets of the enterprise must be clearly identified, their inventory description must be drawn up and maintained. And also that the company should document all assets and outline their importance. It is noted that the inventory description of the enterprise's assets should contain all the information necessary for disaster recovery, including the type of asset, format, location, backup and license information, and business value. The inventory description should not duplicate other descriptions, but their content must be consistent. Considerable attention is paid to the importance of classification of information to identify the need, priority and expected degree of protection during its processing.

The author states that information should be classified in terms of its value, legal requirements, sensitivity and criticality for the enterprise. And also the determined level of information protection can be evaluated by analyzing the confidentiality, integrity, availability and any other requirements for the information in question.

It is noted that information handling procedures should be defined for each classification level, covering secure processing, storage, transmission, declassification (declassification) and destruction. They should also include procedures for the chain of custody and the recording of any safety-critical event.

It is determined that agreements with other organizations, which cover the joint use of information, must contain procedures for identifying the classification of such information and interpreting the classification marks of other organizations. Marking and secure handling of classified information is a key requirement of information sharing agreements. Physical marks are a commonly accepted form of marking. However, some information assets, such as documents in electronic form, cannot be physically marked and require the use of electronic means of marking

It was emphasized that for all assets their owners should be identified and responsibility for maintaining proper controls should be established.

Key words: information protection, enterprise assets, classification of information, classification of enterprise assets.

Сьогодні практично всі підприємства піддаються технологічним загрозам безпеки. Тому багато створюються сучасні засоби захисту, які здатні боротися з атаками кіберзлочинців. Але в сучасному світі цього недостатньо, тому підприємства намагаються створювати такі умови політики безпеки, щоб якого можна значно зменшити ці загрози. Для того щоб забезпечити безпеку підприємства і врахувати, що захист інформації підприємства є дуже складний процес, на підприємствах створюються служби захисту інформації. В службу захисту інформації запрошують на роботу висококваліфікованих фахівців, які можуть застосувати на підприємстві систему управлення інформаційною безпекою. Система управління інформаційною безпекою підприємства – це основа політики підприємства і його засобів, що систематично управляють інформаційною безпекою на упередження ризиків на підприємстві. Для забезпечення системи управляння інформаційної безпеки необхідно для початку класифікувати і організувати захист активів підприємства.

Зважаючи на вище викладене, система управління інформаційною безпекою можлива тільки за умови підтримки та забезпечення умов внутрішньої політики інформаційної безпеки, яка діє на підприємстві. Вивченням питання системи управління інформаційної безпеки на підприємстві займались такі вчені, як: А. М. Гребенюк, Л. В. Рибальченко, А. І. Марущак та інші.

Але на сьогодні ще залишаються не вирішенні питання щодо організації системи управління інформаційної безпеки на підприємстві.

Мета статті є дослідження організації захисту активів підприємства, а також їх класифікація.

Досягти та підтримувати належний захист активів підприємства є важливою та необхідною умовою забезпечення діяльності будь-якого підприємства. На підприємстві існує багато типів активів:

1. інформація: бази даних та файли даних, контракти та угоди, системна документація, дослідницька інформація, настанови для користувачів, навчальний матеріал, процедури функціонування або підтримки, плани безперервності бізнесу, заходи щодо його відновлення, журнали аудиту та архівна інформація;
2. програмні активи: прикладне програмне забезпечення, системне програмне забезпечення, засоби розробки та утиліти; фізичні активи: комп'ютерне обладнання, телекомунікаційне обладнання, замінювані носії та інше обладнання;
3. послуги: обчислювальні та телекомунікаційні послуги, комунальні послуги, наприклад, опалення, освітлення, енергопостачання та кондиціювання повітря;

люди та їх кваліфікація, навички та досвід; нематеріальні активи, такі як репутація та імідж організації.

Усі активи підприємства необхідно чітко ідентифікувати та скласти і підтримувати інвентарний опис.

Інвентарні описи активів підприємства допомагають забезпечити наявність ефективного захисту активів підприємства, а також можуть бути потрібними для інших бізнес-цілей, наприклад таких як здоров'я та безпека, страхові або фінансові причини. Процес складання інвентарного опису активів підприємства є важливою передумовою управління ризиком.

Підприємство повинно ідентифікувати всі активи і задокументувати важливість цих активів. Інвентарний опис активів підприємства повинно містити всю інформацію, необхідну для відновлення після лиха, в тому числі, тип активу, формат, розташування, резервну та ліцензійну інформацію та бізнес-цінність. Інвентарний опис не повинен дублювати інші описи, проте треба гарантувати узгодженість їх змісту.

Для того щоб забезпечити, щоб інформація мала належний рівень захисту, тому інформація повинна бути класифікована для ідентифікації потреби, пріоритетності та очікуваного ступеня захисту під час її оброблення.

Інформація має різні ступені чутливості та критичності. Деякі елементи можуть потребувати додаткового рівня захисту або певного оброблення. Схема класифікації інформації повинна використовуватися для визначення відповідного набору рівнів захисту і зв'язку з потребою в спеціальних заходах поводження з інформацією.

Інформація повинна бути класифікована в термінах її цінності, правових вимог, чутливості та критичності для підприємства.

Класифікація та пов'язані з нею контролі захисту інформації повинні брати до уваги бізнес-потреби для спільного використання або обмеження інформації та бізнес-впливи, пов'язані з такими потребами.

Настанови щодо класифікації повинні містити домовленості щодо первинної класифікації та повторної класифікації через певний час, відповідно до заздалегідь визначеній політиці контролю доступу.

Повинна бути встановлена відповідальність власника активу за визначення класифікації активу, періодичний її перегляд, забезпечення підтримки її в актуальному стані і на відповідному рівні.

Треба розглянути кількість класифікаційних категорій і переваг, які будуть отримані від їх використання. Надмірно складні схеми можуть стати громіздкими й неекономічними для використання або виявитися непрактичними. Треба потурбуватися щодо інтерпретації класифікаційних позначок на документах з інших організацій, які можуть мати інші визначення для тих самих або аналогічно названих позначок.

Рівень захисту може бути оцінений шляхом аналізу конфіденційності, цілісності, доступності та будь-яких інших вимог до розглядуваної інформації.

Інформація часто перестає бути чутливою або критичною після певного періоду часу, наприклад, після того, як інформація стає загальнодоступною. Ці аспекти треба взяти до уваги, оскільки надмірна класифікація може призвести до впровадження непотрібних контролів, наслідком яких будуть додаткові витрати.

Розгляд документів зі схожими вимогами безпеки під час призначення класифікаційних рівнів може допомогти у спрощенні задачі класифікації.

Взагалі, класифікація, яка надана інформації, є коротким шляхом визначення того, як ця інформація повинна оброблятися та захищатися.

Належна множина процедур для маркування та оброблення інформації повинна бути розроблена та впроваджена згідно зі схемою класифікації, прийнятою на підприємстві.

Необхідно, щоб процедури маркування інформації поширювалися на інформаційні активи в матеріальному та електронному вигляді.

Вихідні дані систем, які містять інформацію, класифіковану як чутлива або критична, повинні містити відповідну класифікаційну позначку (на виході). Маркування повинне відображати класифікацію відповідно до встановлених правил. Розглядуваними елементами є надруковані звіти, екрани дисплеїв, носії записів (наприклад, флеш пам'ять, CD), електронні повідомлення та обмін файлами.

Для кожного класифікаційного рівня повинні бути визначені процедури поводження з інформацією, охоплюючи безпечну обробку, зберігання, передавання, розкласифікацію (виведення з класифікації) та знищення. Вони повинні містити також процедури для ланцюга охорони та реєстрації будь-якої події, суттєвої для безпеки.

Угоди з іншими організаціями, які охоплюють спільне використання інформації, повинні містити процедури ідентифікації класифікації такої інформації та інтерпретації класифікаційних позначок інших організацій.

Маркування та безпечне оброблення класифікованої інформації є ключовою вимогою угод щодо спільного використання інформації. Фізичні позначки є загальноприйнятою формою маркування. Проте, деякі інформаційні активи, такі як документи в електронному вигляді, не можуть бути фізично позначені і потребують використання електронних засобів маркування. Наприклад, позначка сповіщення може з'являтися на екрані або дисплеї. Там, де позначки зробити неможливо, можуть бути застосовані інші засоби позначення класифікації інформації, наприклад, через процедури або метадані.

Вся інформація і активи, пов'язані із засобами оброблення інформації, повинні «бути у власності» визначеного підрозділу підприємства.

Усі активи повинні бути враховані та мати призначеного власника.

Для всіх активів повинні бути ідентифіковані їх власники і повинна бути встановлена відповідальність за підтримування належних контролів. Впровадження певних контролів може делегуватися власником, якщо це прийнятно, проте відповідальним за належний захист активів залишається власник. Термін «власник» ідентифікує особу, відділ підприємства або організацію, для якої встановлено затверджену керівництвом відповідальність щодо контролювання виробництва, розвитку, підтримування, використання та безпеки активів. Термін «власник» не означає, що особа дійсно має права власності на актив підприємства.

Власник активів повинен бути відповідальний за:

– забезпечення того, що інформація та активи, пов'язані з засобами оброблення інформації, відповідним чином класифіковані;

– визначення та періодичний перегляд обмежень та класифікації доступу, беручи до уваги застосовну політику контролю доступу.

Висновки.

Підсумовуючи, що класифікація та організація стратегій захисту активів підприємства вимагають комплексного та багатогранного підходу. Розуміючи різні категорії активів і впроваджуючи відповідні заходи захисту, підприємства можуть зменшити ризики, запобігти втратам і підтримувати безперервність роботи. Постійні дослідження, адаптація до нових загроз і проактивне мислення є важливими для ефективного захисту активів у сучасному динамічному бізнес-ландшафті.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Методи захисту системи управління інформаційною безпекою. Вимоги. [Чинний від 01.01.2017]. Київ, 2016. 28 с. (ДП «УкрНДНЦ»).

2. Андрєєв В.І., Козюра В.Д., Скачек Л.М., Хорошко В.О. Стратегія управління інформаційною безпекою. К.: ДУІКТ, 2008. 277 с.