2. Advantages of Gantt Charts in Project Planning URL: https://business.adobe.com/blog/basics/what-is-a-gantt-chart (дата звернення: 21.10.2024).
3. 25 Best Free Project Management Software: Tools to Try in URL: https://clickup.com/blog/free-project-management-software/ (дата звернення: 21.10.2024).

DOI https://doi.org/10.30525/978-9934-26-506-8-105

THE PROCESS OF INVENTORYING CRITICAL INFORMATION AT THE ENTERPRISE

ПРОЦЕС ІНВЕНТАРИЗАЦІЇ КРИТИЧНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Ilchenko M.V.,
Head of the Information Protection Department, LLC Metinvest digital , Student (group 122-23-1м), LLC "Technical university "Metinvest polytechnic", Zaporizhzhia, Ukraine

Ільченко М.В.,
начальник відділу захисту інформації, ТОВ «Метінвест діджитал», студент гр. 122-23-1м, ТОВ «Технічний університет «Метінвест політехніка», м. Запоріжжя, Україна

Sahaida P.I.,
DSc (Engineering), Associate Professor, LLC "Technical university "Metinvest polytechnic", Zaporizhzhia, Ukraine

Сагайда П.І.,
д.т.н., доцент, ТОВ «Технічний університет «Метінвест політехніка», м. Запоріжжя, Україна

В умовах швидкого розвитку технологій та зростання кількості кібератак сучасні підприємства стикаються з необхідністю забезпечення кіберстійкості. Одним з важливих елементів цього процесу є інвентаризація критичної інформації. Процес інвентаризації дозволяє виявити та класифікувати інформаційні активи (форму в якій обробляється інформація), що є критично важливими для підприємства, а також ідентифікувати потенційні ризики та загрози для їх безпеки. Процес необхідний для ефективного управління інформаційною безпекою, збереженням даних та їх плануванням їх захисту, зменшенням

ризиків впливу на репутацію компанії, довіри клієнтів та партнерів, а також її фінансової стабільності.

Одним з ключових аспектів інвентаризації критичної інформації є її відповідність міжнародним стандартам, таким як ISO/IEC 27001:2022. Цей стандарт надає керівництво щодо встановлення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS). Відповідність стандартам ISO дозволяє підприємствам організувати процеси інвентаризації та управління ризиками більш структуровано, що сприяє підвищенню загальної ефективності системи безпеки. Крім того, наявність сертифікації ISO 27001 може бути додатковою перевагою при співпраці з партнерами та клієнтами, оскільки це підтверджує високу якість управління інформаційною безпекою на підприємстві.

Процес інвентаризації критичної інформації допомагає підприємствам зосередити ресурси на найбільш важливих активах, знижуючи при цьому витрати та підвищуючи ефективність захисту. В умовах обмежених ресурсів та високої конкуренції важливо забезпечити, щоб вкладені в безпеки інвестиції мали максимальний ефект. Автоматизація процесів інвентаризації, впровадження інтелектуальних систем для аналізу та оцінки ризиків, а також інтеграція з іншими системами управління інформаційною безпекою дозволяють підприємствам оптимізувати використання ресурсів та підвищити загальну ефективність роботи.

Інвентаризація критичної інформації включає в себе кілька етапів: виявлення інформаційних активів, їх класифікація, оцінка ризиків та загроз, а також розробка заходів для їх мінімізації (може існувати окремо). Виявлення інформаційних активів передбачає створення повного переліку всіх даних, що є критичними для роботи підприємства. Класифікація інформаційних активів дозволяє визначити їх важливість та пріоритетність, що допомагає у подальшому розподілі ресурсів для їх захисту. Оцінка ризиків та загроз включає в себе аналіз потенційних вразливостей та ймовірності їх реалізації, а також визначення можливих наслідків для підприємства. На основі цього аналізу розробляються заходи для мінімізації ризиків, включаючи впровадження технічних, організаційних та процедурних заходів безпеки.

Розвиток процесу інвентаризації критичної інформації включає кілька ключових напрямків:

– автоматизація збору та обробки даних;

– використання сучасних технологій, таких як машинне навчання та штучний інтелект, для підвищення точності та швидкості процесів інвентаризації;

– впровадження інтелектуальних систем для аналізу та оцінки ризиків, що дозволяють прогнозувати можливі загрози та розробляти заходи для їх запобігання.

Великі підприємства для ефективної обробки цього процесу повинні мати систему, яка буде мати можливість електронно обслуговувати процеси збору та актуалізації інформаційних активів за допомогою розроблених стандартизованих даних з урахуванням сучасних можливостей інтеграцій зі штучним інтелектом. Зв'язок зі штучним інтелектом дасть можливість аналітикам, інформаційній безпеці та бізнес-власникам інформації економити свій час для заповнення і скорочувати загальні терміни процесу.

Висновки. В умовах постійних кібератак та зростання вимог до захисту даних, процес інвентаризації критичної інформації стає невід'ємною частиною системи управління інформаційною безпекою. Відповідність міжнародним стандартам, таким як ISO/IEC 27001:2022, підвищує довіру до підприємства та дозволяє забезпечити високу якість захисту інформації. Автоматизація процесів та впровадження сучасних технологій дозволяють значно підвищити ефективність та знизити витрати на забезпечення безпеки. Інвентаризація критичної інформації допомагає підприємствам не лише краще захищати свої дані, але й оптимізувати використання ресурсів та підвищити загальну ефективність роботи.

Перелік використаних джерел

1. ISO/IEC 27001:2022 – Міжнародний стандарт управління інформаційною безпекою. URL: https://www.iso.org/isoiec-27001-information-security.html (дата звернення: 25.10.2024).