УДК 04.056

Радецька А. О.

ВИЗНАЧЕННЯ ЗАХОДІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА НА ОСНОВІ СТРАНДАРТУ ISO 27002

Вінницький національний технічний університет

Анотація

У даній роботі наведено опис можливих заходів та засобів управління що використовуються для організації системи управління інформаційною безпекою, яка відповідає вимогам стандарту ISO 27002. Дані засоби дозволяють значно покращити рівень інформаційної безпеки підприємства та забезпечити організацію його систем та процесів роботи відповідно до вимог серії стандартів ISO 27000.

Ключові слова: ISO 27002, заходи управління, інформаційна безпека, серія стандартів ISO 27000, захист інформації.

Abstract

This paper describes possible measures and controls used to organize an information security management system that meets the requirements of ISO 27002. These tools can significantly improve the level of information security of the enterprise and ensure the organization of its systems and processes in accordance with the requirements of the ISO 27000 series of standards.

Keywords: ISO 27002, management measures, information security, ISO 27000 series of standards, information protection.

Вступ

Сьогоднішній світ характеризується стрімким розвитком технологій, підвищеним обсягом цифрових даних та швидким впровадженням цифрових платформ. У зв'язку з цим зростає кількість кібератак, витоків конфіденційної інформації та інших загроз, що ставлять під загрозу інформаційну безпеку підприємств [1]. Кіберзлочинці намагаються використовувати слабкі місця у системах безпеки для незаконного доступу до конфіденційної інформації, що може призвести до фінансових втрат, порушення репутації, а також втрати довіри клієнтів і партнерів. [2]. Саме тому важливим є організувати побудову інформаційної безпеки на підприємстві таким чином, щоб наявні заходи та засоби захисту ефективно протидіяли усім можливим загрозам. Для цього слід у процесі побудови та реалізації системи захисту використовувати рекомендації та практики, що наведені у стандартах інформаційної безпеки, одним із найкращих у даній сфері є стандарт ISO 27002.

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – є загально визнаним світовою спільнотою фахівців у галузі інформаційної безпеки посібником з вибору та впровадження загальних засобів контролю інформаційної безпеки для зміцнення системи управління інформаційною безпекою. Він містить найкращі практики та вказівки щодо використання цих засобів контролю [3].

Метою роботи є систематизація та визначенні оптимальних заходів управління інформаційною безпекою на основі стандарту ISO 27002 для підприємства. з метою підвищення його інформаційної безпеки та сприяння сталому розвитку.

Результати дослідження

Відповідно до ISO 27002 усі заходи правління інформаційною безпекою поділяються на 4 групи:

- організаційні заходи захисту;
- заходи захисту персоналу;
- фізичні заходи захисту;
- технологічні заходи захисту.

Кожна із категорій охоплює певну частину системи управління інформаційною безпекою та допомагає підприємству організувати максимально можливий рівень захисту.

Організаційні заходи захисту включають в себе різні стратегії, процедури та практики, які допомагають забезпечити безпеку і конфіденційність інформації в організації.

Контроль доступу – це процес управління і регулювання доступу користувачів, пристроїв і систем до інформації та ресурсів в організації. Для його реалізації необхідно запровадити процедури ідентифікації та аутентифікації усіх користувачів систем. Також потрібно реалізувати процедуру управління правами доступу, що включає в себе встановлення ролей та груп доступу для усіх працівників компанії за принципом найменших привілеїв, та їх регулярний перегляд. Необхідно здійснювати моніторинг і аудиту активності користувачів у системах підприємства та фіксувати усі їх дії

Управління інцидентами інформаційної безпеки дозволить організації швидко та своєчасно виявляти та реагувати на виникнення подій, що порушують цілісність, конфіденційність та доступність будь-якої інформації чи системи. Для виявлення інцидентів порушення інформаційної безпеки необхідно використовувати SIEM та IDS/IPS системи. SIEM – це комплексна технологія та підхід до кібербезпеки, що надає організаціям централізовану систему моніторингу, управління та аналізу подій та інформації про безпеку в їхній IT-інфраструктурі [4]. Системи IDS та IPS призначені для виявлення та реагування на інциденти та загрози безпеці в режимі реального часу [5]. Системи IDS генерують сповіщення при виявленні підозрілих дій. Адміністратори безпеки переглядають ці сповіщення, щоб дослідити потенційні загрози. Системи IPS вживають заходів після виявлення загроз.

Заходи захисту персоналу є надзвичайно важливими для організації надійної системи управління інформаційною безпекою. Адже левова частка успішності реалізації СУІБ залежить від того, наскільки працівники компанії обізнані у правилах інформаційної безпеки та дотримуються їх.

Під час проведення процесу найму співробітників необхідно запровадити перевірку на достовірність наданої потенційним кандидатом інформації. Це дозволить уникнути ряду проблем пов’язаних із репутаційними та ресурсними витратами. Перевірка допомагає переконатися, що правильних людей, із належною компетенцією наймають на відповідну роботу.

Усі працівники компанії мають бути ознайомлені із процедурами та правилами політики безпеки. Необхідно запровадити процедуру підписання договорів, у яких чітко буде прописано усі посадові обов’язки працівників, їх рівні доступу до інформації та вказано вимоги щодо нерозголошення конфіденційних даних.

Потрібно запровадити процедуру регулярного проведення навчання та підвищення рівня обізнаності співробітників у галузі інформаційної безпеки. Також необхідно реалізувати процедури контролю отриманих знань та навичок. Для цього можна використати систему тестування або ж усного опитування, ще одним із способів перевірки є створення тестової ситуації порушення інформаційної безпеки, для контролю дій співробітників.

Фізичні заходи захисту стосуються захисту фізичного оточення, де зберігається або оброблюється уся важлива для підприємства інформація.

Для реалізації фізичного захисту необхідно здійснити контроль доступу на територію та до приміщень організації. Для цього необхідно забезпечити наявність контрольованих зон за допомогою систем відеоспостереження, сигналізацій, пропускних карток та перепусток.

Доступ до серверів та комунікаційного обладнання потрібно обмежити шляхом їх розміщення у спеціальних закритих приміщеннях, або ж у спеціальних коробах та захисних ящиках. Доступ до них повинен бути лише у обмеженого кола осіб, у чиї посадові обов’язки входить робота з даним видом обладнання.

Слід впровадити необхідні запобіжні заходи, щодо мінімізації ризиків, що пов’язані із загрозами фізичній безпеці від навколишнього середовища. Для мінімізації наслідків пожежі потрібно встановити та налаштувати системи, здатні виявляти пожежі на ранній стадії та надсилати сигнали тривоги або запускати системи пожежогасіння. Для захисту від повені чи підтоплення слід здійснити встановлення систем, здатних виявляти затоплення на ранній стадії під підлогою зон, що містять носії інформації або системи обробки інформації. Водяні насоси або еквівалентні засоби повинні бути наявними та легкодоступними на випадок затоплення. Для захисту від загроз, пов’язаних електроенергією потрібно встановити системи безперебійного аварійного живлення та захисту від стрибків напруги.

Потрібно запровадити політику чистого столу та екрану. Всі співробітники мають залишали свої робочі столи чистими і порожніми після завершення робочого. Необхідно прибрати зі столу всі документи, записи, ключі, карти доступу та інші матеріали, які можуть містити конфіденційну інфор-

мацію. Після завершення робочого сеансу слід блокувати екран або вимикати комп'ютер. Важливо забезпечити фізичний захист документів, для цього їх необхідно зберігати у закритих шафах або сейфах.

Технологічні заходи захисту спрямовані на захист інформаційних активів організації від різних технологічних загроз і вразливостей.

За допомогою криптографічних методів реалізується захист конфіденційності, цілісності та достовірності інформації. До них відноситься використання процесу шифрування даних, що передаються або ж зберігаються у інформаційних системах підприємства та цифрових підписів для перевірки автентичності та цілісності.

Для забезпечення мережевої безпеки необхідно використовувати брандмауери, системи виявлення та запобігання вторгненням, сканери мережевої активності а також сегментацію мережі. Брандмауери діють як бар'єр між надійною внутрішньою мережею та ненадійними зовнішніми мережами, такими як Інтернет. Вони перевіряють і контролюють вхідний і вихідний мережевий трафік на основі політики безпеки організації [6]. Мережеві сканери – це інструменти та програмні додатки, призначені для сканування та оцінки безпеки комп'ютерних мереж, систем і пристроїв [7]. Вони відіграють вирішальну роль у виявленні вразливостей, неправильних конфігурацій і потенційних слабких місць в інфраструктурі мережі. Сегментація мережі дозволить зменшити ризик для несанкціонованого доступу під час мережевих атак.

Необхідно здійснити реалізацію захисту від шкідливого програмного забезпечення, такого як віруси, хробаки, трояни та інше шкідливе програмне забезпечення. Для цього слід забезпечити наявність на усіх пристроях підприємства встановленого антивірусного програмного забезпечення. Необхідно здійснювати регулярне сканування на наявність шкідливого програмного забезпечення усіх файлів та програм, що передаються та надсилаються у мережі компанії.

Необхідно здійснювати виявлення технічних вразливостей у встановлених операційних системах та програмному забезпечені. Для цього слід запровадити використання сканерів вразливостей та здійснення регулярного тестування на проникнення. Сканери вразливостей – це автоматизовані інструменти, які використовуються для виявлення, оцінки та повідомлення про потенційні вразливості безпеки в комп'ютерних системах, мережах і додатках [8]. Ці інструменти відіграють вирішальну роль у підтримці та посиленні інформаційної безпеки організації шляхом виявлення слабких місць, які можуть бути використані зловмисниками. Тестування на проникнення – це процес оцінки безпеки, в якому фахівці з кібербезпеки імітують реальні кібератаки на інформаційні системи, додатки та мережі організації з метою виявлення вразливостей і слабких місць [9]. Основна мета тестування на проникнення – оцінити безпеку активів та інфраструктури організації шляхом імітації зловмисних дій хакерів.

Для запобіганню витоку конфіденційних та критично важливих даних слід впровадити використання DLP рішень. DLP (Data Loss Prevention) – інструменти та рішення для запобігання втраті даних покликані допомогти організаціям запобігти несанкціонованому розкриттю конфіденційної інформації та запобігти витоку даних [10]. Рішення DLP необхідні для захисту конфіденційної інформації, такої як дані клієнтів, інтелектуальна власність, фінансова звітність та інші конфіденційні дані. Вони пропонують широкий спектр можливостей, включаючи виявлення даних, моніторинг, забезпечення дотримання правил та реагування на інциденти.

Для збереження цілісності та доступності інформації слід запровадити виконання процедури резервного копіювання даних. Копіювання даних слід здійснювати регулярно для всіх критичних інформаційних систем та даних. Необхідно забезпечити безпечне та захищене зберігання резервних копій даних від фізичних і кіберзагроз. Усі скопійовані дані мають зберігатися у зашифрованому вигляді. Доступ до резервних копій потрібно забезпечити лише авторизованим співробітникам.

Необхідно встановити контроль над кінцевими точками та способами віддаленого підключення до мережі та систем підприємства. Під кінцевими точками в цьому контексті зазвичай маються на увазі окремі пристрої, такі як робочі станції, ноутбуки, сервери та мобільні пристрої в мережі організації. Для забезпечення безпеки кінцевих точок слід використовувати технологію EDR. EDR (Endpoint Detection and Response) – це технологія і підхід до кібербезпеки, спрямовані на виявлення, розслідування та реагування на інциденти безпеки на рівні кінцевих точок [11]. Рішення EDR призначені для забезпечення видимості в реальному часі діяльності кінцевих точок, виявлення потенційних загроз і швидкого реагування на інциденти. Для віддаленого підключення до мережі підприємства слід вико-

ристовувати VPN [12]. Технологія VPN використовується для забезпечення безпечного та зашифрованого з'єднання, тим самим гарантуючи конфіденційність при передані інформації.

Висновки

ISO 27002 – визнаний міжнародний стандарт у сфері управління інформаційною безпекою. Впровадження заходів, які відповідають цьому стандарту, сприяє встановленню найкращих практик та стандартів у сфері безпеки. За їх допомогою можна уникнути зловмисних дій, кібератак, витоків даних та інших форм порушень безпеки, а також забезпечити захист конфіденційності, цілісності та доступності інформації. Дані заходи захисту являються ефективними засобами управління інформаційною безпекою та допомагають зберегти довіру клієнтів та партнерів. Заходи інформаційної безпеки також сприяють збільшенню ефективності та продуктивності роботи. Вони дозволяють уникнути втрати часу та ресурсів через відновлення даних та працездатності систем, після кібератак та інших інцидентів безпеки, а також допомагають захистити системи та бізнес-процеси від порушень та втрат.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Global number of cybercrime incidents by industry and organization size. Ststista, 2023. URL: https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/ (дата звернення: 30.09.2023)
2. Beamer T. What Industries Are Most Vulnerable to Cyber Attacks In 2022. Tech Business News. 2023. URL: https://www.techbusinessnews.com.au/ what-industries-are-most-vulnerable-to-cyberattacks-in-2022/ (дата звернення: 30.09.2023)
3. ISO/IEC 27002:2022. ISO. URL: https://www.iso.org/standard/75652.html (дата звернення: 30.09.2023).
4. What is SIEM?.IBM. URL: https://www.ibm.com/topics/siem (дата звернення: 02.10.2023).
5. Intrusion Detection and Prevention System. Spiceworks. URL: https://www.spiceworks.com/it-security/vulnerability-management/articles /what-is-idps/ (дата звернення: 02.10.2023).
6. What is a Firewall?. Checkpoint. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ (дата звернення: 02.10.2023).
7. Network Scanning Tools. Intellipaat. URL:https://intellipaat.com/blog/ network- scanning-tools/ (дата звернення: 03.10.2023).
8. Vulnerability Scanning Tools. OWASP. URL: https://www.cshub.com/security-strategy/articles/utilizing-cyber-security-standards-and-frameworks (дата звернення: 03.10.2023).
9. Penetration Testing. Penetration Testing. URL: https://www.synopsys.com/glossary/what-is-penetration-testing.html (дата звернення: 03.10.2023).
10. Data Loss Prevention. Netskope. URL: https://www.netskope.com/security-defined/what-is-data-loss-prevention-dlp (дата звернення: 03.10.2023).
11. Endpoint Detection and Response (EDR) Tools. Cynet. URL: https://www.cynet.com/endpoint-protection-and-edr/top-6-edr-tools-compar ed/ (дата звернення: 03.10.2023)
12. What Is a Virtual Private Network (VPN)?. CISCO. URL: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (дата звернення: 03.10.2023)

Радецька Анастасія Олександрівна – студентка групи 2БС-22м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: an.radetska@gmail.com

Radetska Anastasiia O. – student of group 2BS-22m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: an.radetska@gmail.com