Секція 1

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ПІДПРИЄМСТВА

Марченко В. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Дослідження та розробка політики безпеки виробничого підприємства мають велику актуальність у сучасних умовах. Забезпечення безпеки на робочому місці як складової частини політики безпеки є одним із головних пріоритетів для будь-якого підприємства. Ось декілька причин, чому актуальність досліджень та розробки політики безпеки виробничого підприємства постійно зростає. Оптимізація витрат: Несприятливі події, пов'язані з безпекою, можуть призвести до значних фінансових втрат для підприємства. Наприклад, штрафи за порушення норм безпеки, виплати компенсацій працівникам через травми або хвороби, втрати виробництва через припинення роботи - все це може негативно вплинути на фінансовий стан підприємства. Дослідження та розробка політики безпеки дозволяють підприємству ідентифікувати потенційні ризики та приймати заходи для їх запобігання, що допомагає знизити витрати, пов'язані з безпекою. Збереження репутації: Підприємство, яке піклується про безпеку своїх працівників, буде мати кращу репутацію серед споживачів, інвесторів та інших зацікавлених сторін. Зацікавлені сторони все більше уважають питання безпеки як важливий аспект діяльності підприємства, тому вони активно стежать за тим, як виробничі підприємства впроваджують політику безпеки. Дослідження та розробка політики безпеки допомагають підприємству зберегти свою репутацію і впевненіше працювати на ринку.

Отже, дослідження та розробка політики безпеки виробничого підприємства мають велику актуальність і допомагають забезпечити безпеку працівників, підвищити продуктивність, знизити витрати та зберегти репутацію підприємства.

Мета дослідження та розробки політики безпеки підприємства полягає у створенні ефективної системи заходів та стратегій, спрямованих на забезпечення безпеки підприємства.

Основні положення дослідження та розробки політики безпеки підприємства буде включати наступні елементи. Оцінка загроз: Першим кроком є проведення оцінки загроз, яка включає ідентифікацію потенційних ризиків безпеки, таких як фізична вторгнення, кібератаки, природні катастрофи тощо. Дослідження дозволяє встановити, які загрози є найбільш імовірними і які можуть нанести найбільші збитки підприємству. Аналіз потенційних наслідків: Дослідження повинне включати аналіз можливих наслідків, які можуть виникнути внаслідок

зазначених загроз. Це можуть бути фінансові втрати, порушення конфіденційності даних, втрата репутації підприємства, порушення робочого процесу та інші наслідки. Визначення цілей безпеки: Після оцінки загроз і аналізу наслідків підприємство повинно визначити свої цілі безпеки. Це можуть бути, наприклад, забезпечення безпеки працівників, захист конфіденційності клієнтської інформації, зменшення ризику втрати даних тощо. Розробка стратегій та політик безпеки: Дослідження допомагає визначити оптимальні стратегії та політики безпеки для підприємства. Це може включати впровадження фізичних заходів безпеки, таких як контроль доступу до приміщень або використання відеоспостереження, а також кіберзаходи, такі як використання міцних паролів, шифрування даних та регулярне оновлення програмного забезпечення.

Висновки. Отже, дослідження та розробка політики безпеки підприємства є необхідними для ефективного управління ризиками, забезпечення відповідності, захисту активів та працівників, а також збереження репутації підприємства.

Список літератури

1. ISO 27001:2013 «Information technology – Security techniques – Information security management systems – Requirements». URL – https://certification.com.ua/iso27001?gclid=Cj0KCQiAr8eqBhD3ARIsAIe-buO231SMy2oO23E7KzrFqXX8mS3f3bH_Q3F8vspzLxqjwOesePgHkUQaAlA8EALw_wcB (дата звернення: 11.10.2023);

2. NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations». URL – https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 11.10.2023);

3. Control Objectives For Information And Related Technology, “COBIT”. *Emirsaleh*. URL – https://emirsaleh.wordpress.com/carrier-path/information-technology-world/control-objectives-for-information-and-related-technology-cobit (дата звернення: 11.10.2023);

4. Krag Brotby. Information Security Governance: A Practical Development and Implementation Approach. John Wiley & Sons Inc, 2009, Page 208.

Відомості про автора

Марченко Віктор Васильович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», viktor.marchenko@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, професор кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu