УДК 339.9
DOI https://doi.org/10.32782/2524-0374/2022-8/85

ОРГАНІЗАЦІЯ ВНУТРІШНІХ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

INTERNAL ORGANIZATION MASURES OF INFORMATION SECURITY OF ENTERPRISE

Шепета О.В., к.ю.н., доцент

Стаття присвячена проблемі сьогодення – організації внутрішніх організаційних заходів інформаційної безпеки підприємства. Автором визначені джерела формування вимог безпеки на підприємстві. Значну увагу приділено оцінці ризиків безпеки підприємства. Зазначено якщо управляти інформаційною безпекою підприємства, обов'язково треба встановити структуру управління для започаткування та контролю впровадження інформаційної безпеки підприємства. Визначене коло суб'єктів, які несуть відповідальність за забезпечення інформаційної безпеки підприємства, а також запропоновані сфери відповідальності суб'єктів. Окреслені фактори, які часто є критичними для успішного впровадження інформаційної безпеки на підприємстві. Зазначено, що для забезпечення внутрішніх організаційних заходів інформаційної безпеки підприємства необхідно забезпечити процес управління авторизацією, використання нових засобів оброблення інформації треба визначити їх та впровадити. Акцентовано увагу, що вимоги щодо конфіденційності або угоди щодо нерозголошення, які відображують потреби підприємства у захисті інформації, повинні бути ідентифіковані та підлягають регулярному перегляду. Також на підприємстві може виникнути необхідність використовувати різні форми угод щодо конфіденційності та нерозголошення за різних обставин. Вказано, що обов'язково керівництво підприємства повинно підлягати незалежному перегляду підходу організації до управління інформаційною безпекою та її впровадження (тобто, цілі контролів, контролі, політики, процеси та процедури інформаційної безпеки) в заплановані терміни або за виникнення значних змін у впровадженій безпеці на підприємстві. Такий незалежний перегляд необхідний для забезпечення подальшої придатності, адекватності та ефективності підходу організації внутрішніх організаційних заходів інформаційної безпеки підприємства.

Ключові слова: інформаційна безпека, підприємство, відповідальність, внутрішні організаційні заходи.

The article is devoted to the problem of the enterprise's information security internal organizational measures. The author identified the enterprise's security requirements sources' formation. Considerable attention is paid to the assessment of enterprise security risks.

It is noted that if the information security of the enterprise is to be managed, it is necessary to establish a management structure for the initiation and control of the enterprise's information security implementation. The range of subjects responsible for ensuring the information security of the enterprise is defined, as well as the proposed spheres of responsibility of the subjects.

The factors that are often critical for the successful information security implementation of at the enterprise are outlined. It is noted that in order to ensure internal organizational information security measures of the enterprise, it is necessary to ensure the authorization management process, the use of new means of information processing must be defined and implemented.

It is emphasized that confidentiality requirements or non-disclosure agreements that reflect the enterprise's information protection needs, should be identified and reviewed regularly. A business may also need to use different forms of confidentiality and non-disclosure agreements under different circumstances.

It is indicated that the enterprise management must be the independent review subject of the organization's approach to information security management and its implementation (that is, the objectives of controls, controls, policies, information security processes and procedures) in the planned terms or for the occurrence of significant changes in the implemented security at the enterprise. Such an independent review is necessary to ensure the further suitability, adequacy and effectiveness of the organization's approach to internal organizational information security measures of the enterprise.

Key words: information security, enterprise, responsibility, internal organizational measures.

Зміни, що відбуваються за останні роки у суспільному житті, політиці, економіці, науковій сфері призводять до значного зростання обсягів інформації. Сьогодні безпеку підприємства не можна гарантувати без використання новітніх технологій. З розвитком конкуренції, в сучасному світі на перший план, в захисті підприємства, виходить інформаційна безпека. Тому знання потенційних загроз, причин та умов скоєння злочинів, з застосуванням новітніх технологій, дозволить працівникам підрозділів служб безпеки підприємств у межах своєї компетенції здійснити заходи, що стануть перешкодою на шляху до зловмисних замахів на інформаційні ресурси та потоки господарюючого суб'єкта. Так, захист інформації обумовлений, якщо органи управління підприємства здатні на відповідних рівнях забезпечити проведення робіт із захисту інформації, а також сформувати ефективну систему контролю за нею. Без організації належного захисту інформаційного середовища неможливо забезпечити інформаційну безпеку підприємства. Тому у зв'язку із численними загрозами інформаційній безпеці актуально питання розгляду і потребує вивчення проблеми організації внутрішніх організаційних заходів інформаційної безпеки підприємства.

У зв'язку з вище вказаним тема дослідження представляється актуальною. Вивченням питання організації інформаційної безпеки підприємства займалися такі вчені, як: Андрєєв В.І., Козюра В.Д., Скачек Л.М., Хорошко В.О. Марущак А.та ін.

Але на сьогодні ще залишаються дискусійні питання щодо організації інформаційної безпеки підприємства.

Мета статті є дослідження основних вимог до організації внутрішніх організаційних заходів інформаційної безпеки підприємства.

Інформаційна безпека – це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес ризику і максимізації рентабельності інвестицій і бізнес можливостей.

Інформаційна безпека досягається впровадженням відповідного набору контролів, тобто засобів управління ризиком, які охоплюють політику, процедури, настанови, практику або організаційні структури, які можуть бути адміністративного, технічного, управлінського або правового характеру. Ці контролі необхідно розробити, впровадити, моніторити, переглядати та, за необхідності, вдосконалювати для гарантування того, що певні безпека та бізнес-цілі організації будуть досягнуті. Це треба виконувати узгоджено з іншими процесами управління бізнесом. Основними джерелами формування вимог безпеки є: джерело, яке отримують з оцінки ризиків для підприємства, беручи до уваги загальну бізнес-стратегію підприємства та цілі. Під час оцінювання ризику ідентифікують загрози активам і оцінюють вразливість та ймовірність подій і визначають величину потенційного впливу; іншим джерелом є правові вимоги, ті, що діють на підставі

закону, нормативні та контрактні вимоги, які підприємство, її торгові партнери, підрядники та постачальники послуг повинні задовольняти, а також їх соціально-культурне середовище; ще одним джерелом є власний набір принципів, цілей та бізнес-вимог щодо оброблення інформації, яке підприємство розробило для підтримки свого функціонування. [2].

Так вимоги безпеки ідентифікуються систематичною оцінкою ризиків безпеки. Витрати на контролі повинні бути збалансовані з бізнес-втратами, які можуть бути наслідком порушень безпеки. Результати оцінки ризику допомагатимуть спрямовувати і визначити відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки і впровадження контролів, вибраних для захисту від цих ризиків. Оцінка ризиків повинна періодично повторюватися для врахування будь-яких змін, які можуть вплинути на результати оцінки ризику.

Як тільки вимоги безпеки та ризики ідентифіковано і рішення щодо оброблення ризиків прийнято, повинні бути вибрані та впроваджені відповідні контролі для забезпечення зниження ризиків до прийнятного рівня. Вони або базуються на основних законодавчих вимогах, або розглядаються як звичайна практика інформаційної безпеки. Контролі, які вважаються суттєвими для організації з законодавчої точки зору, містять, залежно від застосовного законодавства: захист даних та конфіденційність персональної інформації; захист записів підприємства; права інтелектуальної власності [1].

Контролі, які вважаються звичайною практикою інформаційної безпеки, містять: документ політики інформаційної безпеки; розподіл відповідальності щодо інформаційної безпеки; поінформованість, освіта і навчання з інформаційної безпеки; правильне оброблення інформації у прикладних програмах; управління технічною вразливістю; управління безперервністю бізнесу; управління інцидентами інформаційної безпеки та вдосконаленням.

Досвід показує, що нижченаведені фактори часто є критичними для успішного впровадження інформаційної безпеки на підприємстві: політика інформаційної безпеки, цілі та діяльність, які відображують цілі бізнесу; підхід та основні правила впровадження, підтримання, моніторингу та вдосконалення інформаційної безпеки, сумісні з культурою підприємства; очевидна підтримка та зобов'язання керівництва усіх рівнів; добре розуміння вимог інформаційної безпеки, оцінки ризику та управління ризиком; ефективне доведення та роз'яснення інформаційної безпеки до всіх керівників, працівників та інших сторін для досягнення поінформованості; розповсюдження настанов щодо політики інформаційної безпеки та стандартів всім керівникам, працівникам та іншим сторонам; забезпечення фінансування діяльності з управління інформаційною безпекою; забезпечення відповідних поінформованості, навчання та освіти; розроблення ефективного процесу управління інцидентами інформаційної безпеки; впровадження системи вимірювань, яка використовується для оцінювання продуктивності управління інформаційною безпекою і пропозицій зворотного зв'язку для вдосконалення.

Щоб управляти інформаційною безпекою підприємства повинна бути встановлена структура управління для започаткування та контролю впровадження інформаційної безпеки підприємства.

Керівництво повинно затвердити політику інформаційної безпеки, призначити ролі щодо безпеки і координувати та переглядати впровадження безпеки підприємства.

За необхідності, на підприємстві повинно бути створене джерело рекомендацій для фахівців з інформаційної безпеки і забезпечений доступ до нього. Треба розвинути контакти з зовнішніми фахівцями або групами, включаючи відповідні повноважні організації, щоб не відставати від промислових тенденцій, здійснювати моніторинг стандартів та методів оцінки і забезпечити можливість обговорення під час оброблення інцидентів інформаційної безпеки. Необхідно заохочувати багатоплановий підхід до інформаційної безпеки.

Керівництво повинно активно підтримувати безпеку в межах підприємства шляхом чіткого регулювання, підтверджених зобов'язань, чітких призначень та визнання відповідальності за інформаційну безпеку.

Керівництво повинно: забезпечити, щоб задачі інформаційної безпеки були визначені, відповідали вимогам підприємства і були інтегровані у відповідні процеси; сформулювати, переглядати і затверджувати політику інформаційної безпеки; переглядати ефективність впровадження політики інформаційної безпеки; забезпечити чітке регулювання та явну підтримку з боку керівництва ініціативам щодо безпеки; надавати ресурси, потрібні для інформаційної безпеки; затвердити призначення певних ролей і відповідальності стосовно інформаційної безпеки на підприємстві; започаткувати плани та програми підтримки поінформованості щодо інформаційної безпеки; забезпечити, щоб впровадження контролів інформаційної безпеки було скоординоване у межах підприємства.

Керівництво повинно визначити потреби в рекомендаціях внутрішніх та зовнішніх фахівців з інформаційної безпеки і переглядати та координувати результати рекомендацій по всьому підприємству. Залежно від розміру підприємства, такі відповідальності може нести спеціальний керівний форум або існуючий керівний орган, наприклад, рада директорів. Діяльність щодо інформаційної безпеки повинна бути узгодженою між представниками різних підрозділів підприємства з відповідними ролями та посадовими обов'язками.

Зазвичай, координація інформаційної безпеки повинна стосуватися співробітництва і координації спільної діяльності менеджерів, користувачів, адміністраторів, розробників прикладних програм, аудиторів і персоналу безпеки, а також фахівців у таких галузях, як страхування, правові питання, людські ресурси, управління IT або ризиками. Ця діяльність повинна: забезпечити, щоб діяльність з безпеки виконувалася відповідно до політики інформаційної безпеки; визначити, як обробляти невідповідності; затвердити методологію та процеси інформаційної безпеки, наприклад, оцінку ризику, класифікацію інформації; ідентифікувати значні зміни загроз, і також незахищеність від загроз інформації та засобів обробки інформації; оцінити достатність та координувати впровадження контролів інформаційної безпеки; ефективно сприяти в організації освіті, навчанню та поінформованості щодо інформаційної безпеки; виконувати оцінювання інформації, отриманої від моніторингу та перегляду інцидентів інформаційної безпеки, і рекомендувати необхідні дії у відповідь на ідентифіковані інциденти інформаційної безпеки [1].

Якщо підприємство не створює окрему групу з перехресними функціями, наприклад, через те, що така група не відповідає розміру організації, вищеописані дії повинні здійснюватися іншим придатним керівним органом або окремим керівником. Усі відповідальності за інформаційну безпеку треба чітко визначити. Розподіл відповідальності за інформаційну безпеку повинен виконуватися відповідно до політики інформаційної безпеки. Відповідальність за захист окремих активів та за виконання певних процедур безпеки повинна бути чітко ідентифікована. Така відповідальність повинна доповнюватися, за необхідності, більш докладною настановою щодо окремих місць розміщення та засобів обробки інформації. Повинні бути чітко визначені локальні відповідальності щодо захисту активів та виконання певних процедур безпеки, таких як планування безперервності бізнесу.

Особи з визначеними відповідальностями щодо безпеки можуть делегувати задачі безпеки іншим. Незважаючи на це, вони залишаються відповідальними і повинні

визначити, чи всі делеговані задачі виконуються правильно.

Повинні бути чітко встановлені сфери відповідальності окремих осіб; зокрема, повинно мати місце наведене нижче:

a) повинні бути ідентифіковані та чітко визначені активи та процедури безпеки, пов'язані з кожною окремою системою;

b) повинна бути призначена особа, відповідальна за кожний актив чи процедуру безпеки і ці відповідальності повинні бути докладно задокументовані;

c) повинні бути чітко визначені й задокументовані рівні авторизації [1].

У багатьох організаціях керівник з інформаційної безпеки призначається повністю відповідальним за розвиток і впровадження безпеки та за підтримку ідентифікації контролів.

Проте, відповідальність за добір ресурсів та впровадження контролів часто залишається за окремими менеджерами. Звичайною практикою є призначення для кожного активу власника, який внаслідок цього стає відповідальним за щоденний захист активу.

Процес управління авторизацією використання нових засобів оброблення інформації треба визначити та впровадити.

Для процесу авторизації повинні бути розглянуті наведені нижче настанови: нові засоби повинні мати належну авторизацію служби управління користувачами, яка авторизує їх цілі та використання. Авторизацію треба також отримати від керівника, відповідального за підтримку інфраструктури безпеки локальної інформаційної системи для гарантії того, що виконані всі суттєві політики безпеки та вимоги; там, де це необхідно, повинні бути перевірені апаратні засоби та програмне забезпечення, щоб гарантувати їх сумісність з іншими компонентами системи; використання персональних чи приватних засобів обробки інформації, наприклад, портативних, домашніх або кишенькових пристроїв, для обробки бізнес-інформації може спричинити нові вразливості, тому повинні бути ідентифіковані й запроваджені необхідні контролі.

Вимоги щодо конфіденційності або угоди щодо нерозголошення, які відображують потреби організації у захисті інформації, повинні бути ідентифіковані та підлягають регулярному перегляду.

Угоди щодо конфіденційності або нерозголошення повинні враховувати вимоги захисту конфіденційної інформації з використанням існуючих правових норм. Для ідентифікації вимог до угод щодо конфіденційності або нерозголошення треба розглянути наведені нижче елементи: визначення інформації, яка повинна бути захищена (наприклад, конфіденційна інформація); очікувана тривалість угоди, охоплюючи випадки, коли конфіденційність повинна підтримуватися необмежено; необхідні дії після припинення угоди; відповідальності та дії сторін, що підписали угоду, для запобігання неавторизованому розголошенню інформації (типу «необхідно знати»); право власності на інформацію, секрети виробництва та інтелектуальна власність і як вони співвідносяться з захистом конфіденційної інформації; дозволене використання конфіденційної інформації і права сторони, яка підписала угоду, користуватися інформацією; право аудиту і моніторингу діяльності, пов'язаної з конфіденційною інформацією; процес сповіщення та звітування щодо неавторизованого розголошення або порушень конфіденційної інформації; терміни повернення або руйнування інформації у разі припинення угоди та очікувані дії, яких треба вжити у разі порушення угоди. Виходячи з вимог безпеки організації, може виникнути необхідність включати в угоду щодо конфіденційності або нерозголошення також інші елементи. Угоди щодо конфіденційності та нерозголошення повинні відповідати усім існуючим законам та нормам для юрисдикції, де вони використовуються. Вимоги до угод щодо конфіденційності та нерозголошення повинні переглядатись періодично, і у випадках змін, які впливають на ці вимоги. Угоди щодо конфіденційності та нерозголошення захищають інформацію пвдприємства та інформують сторони, які підписали угоди, про їх відповідальність щодо захисту, використання та розголошення інформації лише у відповідальний та авторизований спосіб [1].

На підприємстві може виникнути необхідність використовувати різні форми угод щодо конфіденційності та нерозголошення за різних обставин.

Повинні підтримуватись належні контакти з відповідними повноважними органами. На підприємстві повинні бути наявні процедури, які визначають, коли і з якими повноважними органами (наприклад, органами забезпечення правопорядку, пожежної охорони, наглядовими органами) треба контактувати і як своєчасно звітувати про ідентифіковані інциденти інформаційної безпеки, якщо очікується, що цим можуть бути порушені закони. Підприємству, на яке здійснений напад з Інтернету, можуть знадобитись зовнішні треті сторони (наприклад, Інтернет-провайдер або оператор телекомунікацій) для виконання дій проти джерела нападу. Підтримування таких контактів може бути вимогою щодо підтримки управління інцидентом інформаційної безпеки або безперервності бізнесу та процесу планування дій в надзвичайних ситуаціях. Контакти з регулятивними органами також є корисними для передбачення та підготовки до наступних змін до законів та нормативів, яких повинна дотримуватися організація. Контакти з іншими повноважними органами стосуються підприємств комунального обслуговування, аварійних ситуацій, а також здоров'я та безпеки, наприклад, відділів пожежної охорони (у зв'язку з безперервністю бізнесу), операторів телекомунікацій (у зв'язку з маршрутизацією та доступністю ліній), постачальників води (у зв'язку з охолоджувальними засобами обслуговування обладнання).

Повинні підтримуватись належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об'єднаннями. Членство у групах фахівців з певної проблематики або форумах повинно розглядатись як засіб для: вдосконалення знань щодо найкращих практик та поінформованості щодо суттєвої та найсучаснішої інформації з безпеки; забезпечення того, що розуміння інформаційної безпеки є сучасним та повним; отримання ранніх попереджень із застереженнями, повідомленнями про небезпеку, та кодів оперативного виправлення (patches), які стосуються атак і вразливостей; одержання доступу до рекомендацій фахівців з інформаційної безпеки; спільного користування та обміну інформацією щодо нових технологій, продуктів, загроз або вразливостей; забезпечення можливість обговорення під час роботи з інцидентами інформаційної безпеки.

Для вдосконалення співпраці та координації у питаннях безпеки можуть укладатися угоди щодо спільного використання інформації. Такі угоди повинні ідентифікувати вимоги щодо захисту чутливої інформації.

Підхід підприємства до управління інформаційною безпекою та її впровадження (тобто, цілі контролів, контролі, політики, процеси та процедури інформаційної безпеки) підлягають незалежному перегляду в заплановані терміни або за виникнення значних змін у впровадженій безпеці.

Незалежний перегляд повинен ініціюватися керівництвом. Такий незалежний перегляд необхідний для забезпечення подальшої придатності, адекватності та ефективності підходу підприємства до управління інформаційною безпекою. Перегляд повинен охоплювати оцінку можливостей вдосконалення та необхідності змін у підході до безпеки, охоплюючи політику та цілі контролів. Такий перегляд повинен виконуватися особами, незалежними

від переглядувальної області, наприклад, внутрішнім аудитором, незалежним керівництвом або організацією третьої сторони, яка спеціалізується на таких переглядах. Особи, які здійснюють такий перегляд, повинні мати відповідні навички та досвід. Результати незалежного перегляду повинні реєструватися та звітуватися керівництву, яке ініціювало перегляд. Ці записи повинні зберігатися та підтримуватися. Якщо незалежний перегляд виявив, що підхід організації та впровадження управління інформаційною безпекою є неадекватним або невідповідним напряму інформаційної безпеки, встановленому в документі щодо політики інформаційної безпеки, керівництво повинне розглянути коригувальні заходи [1].

Висновки. Отже, сукупність заходів та встановлення структури управління для започаткування та контролю впровадження інформаційної безпеки на підприємстві, це є неодмінна умова якісної організації внутрішніх організаційних заходів інформаційної безпеки на підприємстві.

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.