УДК 339.9
DOI https://doi.org/10.32782/2524-0374/2022-10/128

ОРГАНІЗАЦІЯ ЗАХОДІВ БЕЗПЕКИ ПІДПРИЄМСТВА У ВЗАЄМОДІЇ ІЗ ЗОВНІШНІМИ СТОРОНАМИ

THE ENTERPRISE'S SECURITY MEASURES ORGANIZATION WITHIN EXTERNAL PARTIES INTERACTION

Шепета О.В., к.ю.н., доцент

У статті розглянуті організаційні заходи безпеки підприємства у взаємодії із зовнішніми сторонами. Автором окреслені ризики для інформації підприємства та її засобів оброблення інформації бізнес-процесів, до яких залучені зовнішні сторони. Значну увагу приділено доступу зовнішніх сторін до інформації підприємства, який не повинен надаватися доки не впроваджено відповідні контролі та, де це можливо, не підписано контракт, який визначає терміни та умови підключення або доступу та робочі заходи, а також всі вимоги безпеки, які є наслідком роботи з зовнішніми сторонами або внутрішніми контролями, повинні бути відображені в угоді з зовнішньою стороною.

Вказано, що підприємство може наражатися на ризики, пов'язані з міжорганізаційні процесами, управлінням та зв'язками, якщо має місце високий ступінь аутсорсингу або якщо залучено декілька зовнішніх сторін. А також, що контроль з врахування безпеки під час роботи з клієнтами та контроль врахування безпеки в угодах з третьою стороною стосуються різних угод із зовнішніми сторонами. Визначені вимоги безпеки до процедури надання клієнтам доступ до інформації або активів підприємства.

Зазначено, що обов'язково щодо врахування безпеки в угодах з третьою стороною необхідно врахувати, що угоди з третіми сторонами щодо доступу, оброблення, передавання або управління інформацією організації або засобами оброблення інформації, або щодо до додавання продуктів чи послуг до засобів оброблення інформації повинні охоплювати усі відповідні вимоги безпеки.

Акцентовано увагу, що для різних організацій та різних типів третіх сторін угоди можуть значно відрізнятися. Тому треба звернути увагу на охоплення угодою всіх ідентифікованих ризиків і вимог безпеки. Якщо необхідно, у плані управління безпекою можуть бути розширені необхідні контролі та процедури. Якщо управління безпекою здійснюється на умовах аутсорсингу, угода повинна враховувати, яким чином третя сторона гарантуватиме, що відповідна безпека, визначена оцінкою ризику, буде підтримуватися, і яким чином буде пристосовуватися безпека, щоб ідентифікувати та розглядати зміни ризиків.

Ключові слова: захист інформації, підприємство, ризики, угода, управління безпекою.

The article examines organizational security measures of the enterprise in interaction with external parties. The author outlines the risks for the company's information and its means of information processing of business processes in which external parties are involved. Considerable attention is paid to external party access to enterprise information, which should not be granted until appropriate controls are in place and, where possible, a contract is signed that defines the terms and conditions of connection or access and work arrangements, as well as all security requirements that are the result of the work with external parties as well as internal controls, should be reflected in the agreement with the external party.

It is indicated that the enterprise may be exposed to risks related to inter-organizational processes, management and communications if there is a high degree of outsourcing whether several external parties are involved. And also studied that customer security controls and third-party security controls apply to different third-party deals. security requirements for the procedure of providing clients with access to information or company assets are defined.

It is noted that it is mandatory to consider security in agreements with a third party, it is necessary to take into account that agreements with third parties regarding access, processing, transfer or management of the organization's information or means of information processing, or regarding the addition of products or services to means of information processing must cover all relevant safety requirements.

Attention is drawn to the fact that for different organizations and different types of third parties, agreements may differ significantly. Therefore, it is necessary to pay attention to the coverage of all identified risks and security requirements in the agreement. If necessary, the required controls and procedures can be expanded in the safety management plan. If security management is outsourced, the agreement should consider how the third party will ensure the appropriate security determined by the risk assessment will be maintained as well as how security will be adapted to identify and address risk changes.

Key words: information protection, enterprise, risks, agreement, security management.

На сьогоденному етапі розвитку суспільства, пов'язаного з використанням єдиного інформаційного простору, в рамкам якого відбувається накопичення, обробка, зберігання та обмін інформацією, проблеми організації захисту інформації набувають першочергового значення в усіх сферах суспільної і державної діяльності. Особлива гострота цих проблем на підприємствах визначається такими факторами, як: високими темпами зростання парку інформаційних систем і зв'язку, розширенням сфер використання інформаційних систем, різне та широке застосування інформаційно-керуючих систем, які підлягають сучасного захисту; залученням до процесу інформаційної взаємодії все більшої кількості людей і організацій, а також різким зростанням їх інформаційних потреб; підвищений рівень потреб на інформаційні системи управління і обробки інформації.

Зважаючи на вище викладене, підтримування безпеки інформації організації та її засобів оброблення інформації, до яких мають доступ, обробляють, якими управляють або з якими підтримують зв'язок зовнішні сторони є на сьогодні одним із актуальних питань організації захисту інформації на підприємстві. Вивченням питання організації заходів 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 не вирішенні питання щодо організації захисту інформації підприємства.

Мета статті є дослідження основних вимог до організації заходів безпеки підприємства у взаємодії із зовнішніми сторонами.

Широчезне розповсюджене в даний час поняття інформаційна безпека акцентує важливість організації захисту інформації в сучасному суспільстві і визначає той факт, що інформаційний ресурс зараз має току ж цінність, як виробничі і людські ресурси і так саме підлягає захисту від різного роду посягань, зловживань і злочинів.

Таким чином безпека інформації і засобів оброблення інформації, які належать підприємству, не повинна знижуватись через введення в експлуатацію продуктів або послуг зовнішньої сторони.

Будь-який доступ до засобів оброблення інформації організації, а також оброблення та передавання інформації зовнішнім сторонам повинні бути контрольованими.

Якщо є бізнес-потреба в роботі з зовнішніми сторонами, яка може вимагати доступу до інформації або засобів оброблення інформації підприємства, або в отриманні від зовнішньої сторони чи наданні їй продукту та послуги, повинна виконуватись оцінка ризику для визначення вимог контролю та наслідків щодо безпеки. Контролі

повинні бути погоджені та визначені в угоді з зовнішньою стороною.[2]

Ризики для інформації підприємства та її засобів оброблення інформації бізнес-процесів, до яких залучені зовнішні сторони, повинні бути ідентифіковані і належні контролі повинні бути впроваджені до надання доступу.

Там, де необхідно дозволити зовнішній стороні доступ до засобів оброблення інформації або інформації підприємства, повинна виконуватися оцінка ризику для ідентифікації будь-яких вимог до певних контролів. Ідентифікація ризиків, які стосуються доступу зовнішніх сторін, повинна брати до уваги нижченаведені питання: засоби оброблення інформації, доступу до яких потребує зовнішня сторона; вид доступу, який зовнішня сторона буде мати до інформації та засобів оброблення інформації, наприклад:

1) фізичний доступ, наприклад, до офісів, комп'ютерних кімнат, картотек;

2) логічний доступ, наприклад, до баз даних, інформаційних систем підприємства,

3) наявність зв'язку між мережею підприємства та мережею(ами) зовнішньої сторони, наприклад, постійний зв'язок, віддалений доступ,

4) чи здійснюється доступ на підприємстві чи поза його межами;

цінність та чутливість залученої інформації та її критичність для функціонування бізнесу; контролі, необхідні для захисту інформації, яку не призначено для доступу зовнішніх сторін; персонал зовнішньої сторони, залучений до оброблення інформації підприємства; як підприємство чи персонал, які авторизовані на доступ, можуть бути ідентифіковані, авторизовані, верифіковані, і як часто це потребує повторного підтвердження; різні засоби та контролі, які використовуються зовнішньою стороною під час зберігання, оброблення, доведення до відома, спільного використання та обміну інформації; вплив відсутності доступу за потребою зовнішньої сторони, і введення чи одержання зовнішньою стороною неточної або недостовірної інформації; практика і процедури поводження з інцидентами інформаційної безпеки та потенційними ушкодженнями, а також терміни та умови відновлення доступу зовнішньої сторони у випадку інциденту інформаційної безпеки; правові та нормативні вимоги, інші контрактні зобов'язання суттєві для зовнішньої сторони, які треба взяти до уваги; як можуть вплинути відповідні заходи на інтереси будь-яких інших зацікавлених сторін.

Доступ зовнішніх сторін до інформації підприємства не повинен надаватися доки не впроваджено відповідні контролі та, де це можливо, не підписано контракт, який визначає терміни та умови підключення або доступу та робочі заходи. Як правило, всі вимоги безпеки, які є наслідком роботи з зовнішніми сторонами або внутрішніми контролями, повинні бути відображені в угоді з зовнішньою стороною.

Повинно бути гарантовано, що зовнішня сторона поінформована щодо своїх зобов'язань і приймає обов'язки та відповідальність, пов'язані з доступом, обробленням, доведенням до відома або управлінням інформацією підприємства та засобами оброблення інформації.

Під час виконання робіт з зовнішніми сторонами підприємство повинно впевнитися, що працівники зовнішньої сторони, які безпосередньо виконують дії за визначеною угодою, обізнані в питаннях безпеки поводження з інформацією підприємства, до якої вони можуть мати доступ.

Інформація може бути піддана ризику зовнішніми сторонами з невідповідним управлінням безпекою. Для адміністрування доступу зовнішньої сторони до засобів оброблення інформації контролі повинні бути ідентифіковані та застосовані. Наприклад, якщо є певна потреба конфіденційності інформації, можуть бути використані угоди щодо нерозголошення.

Підприємства можуть наражатися на ризики, пов'язані з міжорганізаційні процесами, управлінням та зв'язками, якщо має місце високий ступінь аутсорсингу або якщо залучено декілька зовнішніх сторін.

Контроль з врахування безпеки під час роботи з клієнтами та контроль врахування безпеки в угодах з третьою стороною стосуються різних угод із зовнішніми сторонами, наприклад, включаючи: постачальників послуг, таких як Інтернет-провайдери, постачальники мережевих послуг, телефонні послуги, послуги обслуговування та підтримки; послуги безпеки, якими управляють; клієнтів; аутсорсинг засобів і/або функцій, наприклад: IT систем, послуг збору даних, функцій центру телефонного обслуговування; консультантів з управління та бізнесу, аудиторів; розробників та постачальників, наприклад: програмного забезпечення та IT систем; послуги з прибирання, харчування та інші аутсорсингові послуги підтримки; тимчасовий персонал, працюючих студентів та інших тимчасових короткострокових працівників.

Такі угоди можуть допомогти знизити ризики, пов'язані з зовнішніми сторонами.

Врахування безпеки під час роботи з клієнтами. Перш ніж надавати клієнтам доступ до інформації або активів підприємства, повинні бути враховані всі ідентифіковані вимоги безпеки.

Повинні бути розглянуті наведені нижче умови для врахування безпеки до надання клієнтам доступу до будь-яких активів підприємства (залежно від типу та ступеня наданого доступу можуть застосовуватися не всі з них): захист активу, включаючи:

1) процедури захисту активів підприємства, охоплюючи інформацію та програмне забезпечення,

2) процедури, які визначають, чи мала місце будь-яка компрометація активів, наприклад: втрата або модифікація даних,

3) цілісність,

4) обмеження щодо копіювання та розголошення інформації;

опис продукції або послуги, які повинні надаватися; різні причини, вимоги та переваги щодо доступу клієнта; політика контролю доступу, яка охоплює:

1) дозволені методи доступу, а також контроль та використання унікальних ідентифікаторів, таких як ID (ідентифікатор) користувача та паролі,

2) процес авторизації доступу та повноважень користувача,

3) положення про те, що всякий нечітко авторизований доступ – заборонено,

4) процедуру відкликання прав доступу або переривання зв'язку між системами;

заходи щодо звітування, сповіщення та розслідування інформаційних неточностей, інцидентів інформаційної безпеки та порушень безпеки; опис кожної послуги, яка повинна бути зроблена доступною; заданий рівень послуг і неприйнятні рівні послуг; право здійснювати моніторинг та відміняти будь-яку діяльність пов'язану з активами підприємства; відповідні зобов'язання підприємства та клієнта; відповідальності стосовно правових питань і як забезпечується задоволення правових вимог, наприклад, законодавства щодо захисту даних, особливо беручи до уваги різні національні правові системи, якщо угода охоплює співпрацю з клієнтами в інших країнах; права інтелектуальної власності (IPR) та призначення авторського права і захист будь-якої спільної роботи.

Вимоги безпеки пов'язані з доступом клієнтів до активів, можуть значно відрізнятися залежно від засобів оброблення інформації та інформації, до яких здійснюватиметься доступ. Ці вимоги безпеки можуть бути враховані з угодах з клієнтом, які містять усі ідентифіковані ризики та вимоги безпеки.

Угоди з зовнішніми сторонами можуть також включати інші сторони. Угоди, які надають доступ зовнішній стороні, повинні містити дозвіл на призначення інших прийнятних сторін і умови їх доступу та залучення.

Врахування безпеки в угодах з третьою стороною щодо доступу, оброблення, передавання або управління інформацією організації або засобами оброблення інформації, або щодо до додавання продуктів чи послуг до засобів оброблення інформації повинні охоплювати усі відповідні вимоги безпеки.

Угода повинна забезпечувати відсутність непорозумінь між підприємством та третьою стороною. Підприємство повинно задовольнити свої інтереси щодо відшкодування збитків третьою стороною.

Щоб задовольнити визначені вимоги безпеки, треба розглянути внесення до угод наведених нижче умов: політики інформаційної безпеки; контролів для забезпечення захисту активів, включаючи: процедури захисту активів організації, включаючи інформацію, програмне забезпечення та апаратні засоби; будь-які необхідні контролі та механізми фізичного захисту; контролі для забезпечення захисту від зловмисного програмного забезпечення; процедури для визначення, чи мала місце якась компрометація активів, наприклад: втрата або модифікація інформації, програмного забезпечення та апаратних засобів; контролі для забезпечення повернення чи знищення інформації та активів по закінченні або в погоджений момент часу протягом дії угоди; конфіденційність, цілісність, доступність та будь-які інші відповідні властивості активів; обмеження щодо копіювання та розголошення інформації та використання угод щодо конфіденційності; навчання користувача та адміністратора щодо методів, процедур та безпеки; забезпечення поінформованості користувача щодо проблем та відповідальності з інформаційної безпеки; умов щодо переміщення персоналу, за необхідності; відповідальності стосовно інсталяції та підтримки апаратних засобів та програмного забезпечення; чіткої структури звітування та погоджених форматів звітування; чіткого та визначеного процесу управління змінами; політики контролю доступу, яка охоплює:

1) різні причини, вимоги та переваги, які роблять доступ третіх осіб необхідним,

2) дозволені методи доступу, контроль та використання унікальних ідентифікаторів, таких як ID користувача та паролі,

3) процес авторизації доступу користувача та повноважень,

4) вимогу щодо підтримки переліку осіб, яким надано право використання доступних послуг, і які права та повноваження цих осіб стосовно такого використання,

5) положення про те, що всякий нечітко авторизований доступ є забороненим,

6) процес відкликання прав доступу або переривання зв'язку між системами;

заходів щодо звітування, сповіщення та розслідування інцидентів інформаційної безпеки та порушень безпеки, а також порушень вимог, встановлених в угоді; опису продукту або послуги, які повинні надаватися, та опис інформації, яка повинна бути доступною, разом з її класифікацією щодо безпеки; заданого рівня послуги і неприйнятні рівні послуги; визначення критеріїв продуктивності, які можуть бути верифіковані, їх моніторинг та звітування; права здійснювати моніторинг та відміняти будь-яку діяльність, яка стосується активів підприємства; права здійснювати аудит відповідальностей, визначених в угоді, мати такі аудити, які виконуються третьою стороною, та перелічувати права аудиторів, що відповідають законодавству; встановлення процесу ескалації для розв'язання проблеми; вимоги безперервності послуги, в тому числі заходи щодо доступності та надійності відповідно до бізнес-пріоритетів підприємства; відповідних зобов'язань сторін угоди; відповідальностей стосовно правових питань і способу забезпечення виконання правових вимог, наприклад: законодавства щодо захисту даних, особливо беручи до уваги різні національні правові системи, якщо угода охоплює співпрацю з клієнтами в інших країнах; права інтелектуальної власності (IPR), визнання авторського права і захисту будь-якої спільної роботи; залучення третьої сторони як субконтрактора і контролі безпеки, які ці субконтрактори повинні запровадити; умов перегляду/припинення угод:

1) наявність на місці плану дій в надзвичайних ситуаціях, якщо якась із сторін бажає припинити відносини до закінчення угоди;

2) перегляд угод за умови зміни вимог безпеки підприємства;

3) поточне документування переліків активів, ліцензій, угод або прав, які їх стосуються.[1]

Висновки. Для різних підприємств та різних типів третіх сторін угоди можуть значно відрізнятися. Тому треба звернути увагу на охоплення угодою всіх ідентифікованих ризиків і вимог безпеки. Якщо необхідно, у плані управління безпекою можуть бути розширені необхідні контролі та процедури.

Якщо управління безпекою здійснюється на умовах аутсорсингу, угода повинна враховувати, яким чином третя сторона гарантуватиме, що відповідна безпека, визначена оцінкою ризику, буде підтримуватися, і яким чином буде пристосовуватися безпека, щоб ідентифікувати та розглядати зміни ризиків.

Різниця між аутсорсингом та іншими формами постачання послуг третьою стороною включає питання відповідальності, планування перехідного періоду і потенційного порушення функціонування протягом цього періоду, заходи з планування дій в аварійних ситуаціях і належні перегляди, збирання та управління інформацією щодо інцидентів безпеки. Тому важливо, щоб підприємство планувало та управляло переходом до аутсорсингових заходів і мало на місцях відповідні процеси для управління змінами та переукладанням/припиненням угод.

Щоб уникнути будь-якої затримки у розміщенні замінюваних послуг, в угоді повинні бути розглянуті процедури для продовження обробки у випадку, коли третя сторона стає нездатною постачати свої послуги.

Угоди з зовнішніми сторонами можуть також залучати інші сторони. Угоди, які надають доступ зовнішній стороні, повинні містити дозвіл на призначення інших припустимих сторін і умови їх доступу та залучення.

Взагалі, угоди спочатку розробляються підприємством. За деяких обставин можуть бути випадки, коли угода може розроблятися і примусово надаватися підприємству третьою стороною. Підприємство повинно забезпечити, щоб вимоги третьої сторони, передбачені в примусово наданих угодах, надмірно не впливали на його власну безпеку.

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.