УДК 339.9
DOI https://doi.org/10.32782/2524-0374/2023-9/71

ПІДБІР ПЕРСОНАЛУ ТА РОБОТА З НИМ В ПИТАННЯХ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

RECRUITMENT OF PERSONNEL AND WORK WITH THEM IN ISSUES PROTECTION OF INFORMATION SECURITY

Шепета О.В., к.ю.н., доцент

У статті розглянуто питання щодо захисту інформаційної безпеки на підприємстві та визначено в роль підбору персоналу на підприємство. Вказано, що система управління інформаційною безпекою можлива тільки за умови підтримки та забезпечення умов внутрішньої політики та якісного підбору персоналу на підприємство. Значну увагу було приділено щодо безпеки та відповідальності, які повинні бути встановлені та чітко доведені до відома претендентів на роботу в процесі, що передує найму.

А також, що службі безпеки підприємства потрібно проводити ретельні перевірки кандидатів на найм, що в себе включає верифікаційні перевірки біографічних даних щодо всіх кандидатів на найм, контракторів та користувачів третьої сторони. Зазначено, що там, де на посаду чи при початковому призначенні, чи при підвищенні по службі залучають осіб, які матимуть доступ до засобів оброблення інформації, і особливо, якщо вони оброблятимуть чутливу інформацію, наприклад, фінансову або конфіденційну інформацію, підприємство повинно передбачити також і подальші більш детальні перевірки. Автором зазначено, що правила та процедури перевірок повинні визначати критерії та обмеження для верифікаційних перевірок, наприклад, хто має право ретельно перевіряти людей і як, коли й чому верифікаційні перевірки проводяться. А також, що інформація щодо всіх кандидатів, які розглядаються для роботи на підприємстві, повинні збиратися та оброблятися згідно з відповідним законодавством, існуючим у відповідній юрисдикції.

Визначено, що частину своїх зобов'язань за контрактом, найманий персонал, контрактори та користувачі третьої сторони повинні погодити і підписати терміни та умови свого контракту з найму, який повинен встановити взаємні відповідальності щодо інформаційної безпеки.

Зазначено, що навчання персоналу заходам захисту інформаційної безпеки відіграє значну роль для поліпшення поінформованості та призначене для того, щоб надати можливість працівникам усвідомити проблеми та інциденти інформаційної безпеки і реагувати згідно з потребами їхніх посадових обов'язків.

Акцентовано увагу, що відповідальність та обов'язки щодо чутливої інформації підприємства повинні міститися у контрактах найманого персоналу, контрактора або користувача третьої сторони після припинення найму.

Ключові слова: підбір персоналу, інформаційна безпека, дисциплінарний процес, верифікаційні перевірки, підприємство.

The article examines the issue of information security protection at the enterprise and defines the role of personnel selection at the enterprise. It is indicated that the information security management system is possible only under the condition of support and ensuring the conditions of internal policy and quality selection of personnel for the enterprise. Considerable attention has been paid to safety and responsibilities, which must be established and clearly communicated to job applicants in the pre-employment process.

And also that the company's security department needs to conduct thorough background checks on potential hires, which includes background checks on all potential hires, contractors and third-party users. It is noted that where persons who will have access to information processing facilities are recruited to the position or upon initial appointment or during promotion, and especially if they will process sensitive information, for example, financial or confidential information, the enterprise must also provide further more detailed checks. The author states that vetting policies and procedures should define the criteria and limitations for verification checks, such as who has the right to thoroughly check people and how, when and why the verification checks are conducted. And also that information about all candidates being considered for positions at the company must be collected and processed in accordance with the relevant laws existing in the relevant jurisdiction.

As part of their contractual obligations, employees, contractors and third-party users must agree to and sign the terms and conditions of their employment contract, which must establish mutual information security responsibilities.

It is noted that awareness training is designed to enable employees to be aware of information security issues and incidents and respond in accordance with the needs of their job duties.

It is emphasized that the responsibilities and obligations that remain in force after the termination of employment should be contained in the contracts of the hired personnel, contractor or third party user.

Key words: personnel selection, information security, disciplinary process, verification checks, corporation.

Сьогодні практично всі підприємства піддаються технологічним загрозам безпеки. Тому багато створюються сучасні засоби захисту, які здатні боротися з атаками кіберзлочинців. Але в сучасному світі цього недостатньо, тому підприємства намагаються створювати такі умови політики безпеки, щоб якого можна значно зменшити ці загрози. Для того щоб забезпечити безпеку підприємства і тому що захист інформації підприємства дуже складний процес, на підприємствах створюються служби захисту інформації. В службу захисту інформації запрошують на роботу висококваліфікованих фахівців, які можуть застосувати на підприємстві систему управлення інформаційною безпекою. Система управління інформаційною безпекою підприємства – це основа політики підприємства і його засобів, що систематично управляють інформаційною безпекою та займаються упередженням ризиків на підприємстві. Для забезпечення системи управляння інформаційної безпеки необхідно визначити організацію управляння матеріальними ресурсами підприємства, а також визначити вимоги для підбору персоналу та роботу з ним в питаннях захисту інформаційної безпеки.

Зважаючи на вище викладене, система управління інформаційною безпекою можлива тільки за умови підтримки та забезпечення умов внутрішньої політики та якісного підбору персоналу на підприємство. Вивченням питання системи управління інформаційної безпеки на підприємстві займались такі вчені, як: Андрєєв В. І., Козюра В. Д., Скачек Л. М., Хорошко В. О. та інші.

Але на сьогодні ще залишаються не вирішенні питання щодо організації якісного підбору персоналу на підприємствах та роботу з ним в питаннях захисту інформаційної безпеки.

Мета статті є дослідження організації управлянням матеріальними ресурсами підприємства, а також вимог для підбору персоналу та роботу з ним в питаннях захисту інформаційної безпеки.

У сучасному бізнес-ландшафті ефективне управління матеріальними ресурсами та надійний захист інформації є вирішальними для успіху та стабільності будь-якого підприємства. Підприємство визнає важливість цих аспектів і прагне оптимізувати свою практику управління та критерії відбору персоналу в цих сферах. Ролі щодо безпеки

та відповідальності визначені та задокументовані відповідно до політики інформаційної безпеки підприємства повинні містити вимоги щодо: впровадження та діяльності згідно з політикою інформаційної безпеки підприємства; захисту активів від неавторизованого доступу, розголошення, модифікації, руйнування або втручання; виконання особливих процедур або дій щодо безпеки; гарантування встановленої для особи відповідальності за здійснювані дії; звітування про події безпеки, або можливі події, або інші ризики безпеки на підприємстві [1].

Ролі щодо безпеки та відповідальності повинні бути встановлені та чітко доведені до відома претендентів на роботу в процесі, що передує найму.

Для документування ролей щодо безпеки та відповідальності можуть бути використані посадові інструкції. Повинні також бути чітко визначені та доведені до відома ролі щодо безпеки та відповідальності осіб, залучених не через процедуру найму на підприємстві, наприклад, найнятих через організацію третьої сторони. Потрібно службі безпеки підприємства провести ретельну перевірку кандидатів на найм, що в себе включає верифікаційні перевірки біографічних даних щодо всіх кандидатів на найм, контракторів та користувачів третьої сторони.

Верифікаційні перевірки повинні враховувати все відповідне законодавство щодо приватності, захисту персональних даних та найму і повинні там, де це дозволено, містити таке: наявність задовільних характеристик, наприклад, одної бізнесової і одної особової; перевірку (на повноту та точність) резюме претендентів; підтвердження заявленої академічної та професійної кваліфікації; незалежну ідентифікаційну перевірку особи; більш детальні перевірки, такі як кредитні перевірки або перевірки за кримінальним обліком.

Там, де на посаду чи при початковому призначенні, чи при підвищенні по службі залучають осіб, які матимуть доступ до засобів оброблення інформації, і особливо, якщо вони оброблятимуть чутливу інформацію, наприклад, фінансову або конфіденційну інформацію, підприємство повинно передбачити також і подальші більш детальні перевірки.

Процедури повинні визначати критерії та обмеження для верифікаційних перевірок, наприклад, хто має право ретельно перевіряти людей і як, коли й чому верифікаційні перевірки проводяться.

Процес ретельної перевірки повинен також проводитися для контракторів і користувачів третьої сторони. Якщо контрактори наймаються через сторонню організацію, угода з цією організацією повинна чітко визначати відповідальність організації за ретельну перевірку та процедури сповіщення, яких вона повинна дотримуватися, якщо ретельну перевірку не було завершено або якщо результати викликають сумнів або занепокоєння. Аналогічно угода з третьою стороною повинна чітко визначати всі відповідальності та процедури сповіщення щодо ретельної перевірки.

Інформація щодо всіх кандидатів, які розглядаються на посади на підприємстві, повинна збиратися та оброблятися згідно з відповідним законодавством, існуючим у відповідній юрисдикції. Залежно від існуючого законодавства кандидати повинні бути наперед поінформовані щодо діяльності і ретельної перевірки.

Як частину своїх зобов'язань за контрактом, найманий персонал, контрактори та користувачі третьої сторони повинні погодити і підписати терміни та умови свого контракту з найму, який повинен встановити взаємні відповідальності щодо інформаційної безпеки.

Терміни та умови найму повинні погоджуватися з політикою безпеки на підприємстві, роз'яснювати та встановлювати: що весь найманий персонал, контрактори та користувачі третьої сторони, яким наданий доступ до чутливої інформації, повинні підписати угоду щодо конфіденційності або нерозголошення до надання доступу до засобів оброблення інформації; правову відповідальність та права найманого персоналу, контракторів та будь-яких інших користувачів, наприклад, стосовно законів про авторське право або законодавства про захист інформації з обмеженим доступом; відповідальності за класифікацію інформації і управління активами підприємства, пов'язаними з інформаційними системами та послугами, з якими має справу найманий персонал, контрактор або користувач третьої сторони; відповідальності найманого персоналу, контрактора або користувача третьої сторони за оброблення інформації, отриманої від інших компаній або зовнішніх сторін; відповідальності підприємства щодо поводження з персональною інформацією, в тому числі персональною інформацією, створеною в результаті або в ході найму на це підприємство; відповідальності поза межами службових приміщень підприємства та поза межами звичайного робочого часу, наприклад, у випадку роботи вдома; дії, яких треба вжити, якщо найманий персонал, контрактор або користувач третьої сторони нехтує вимогами безпеки, які діють на підприємстві.

Підприємство повинно забезпечити, що найманий персонал, контрактори та користувачі третьої сторони згодні з термінами та умовами щодо інформаційної безпеки, які відповідають виду та ступеню доступу, який вони матимуть до активів підприємства, пов'язаних з інформаційними системами та послугами.

Там, де це потрібно, відповідальність, що міститься в термінах та умовах найму, повинна розповсюджуватися на визначений період після закінчення найму.

Можна застосувати кодекс поведінки, щоб охопити відповідальності найманого персоналу, контракторів та користувачів третьої сторони стосовно конфіденційності, захисту даних, етики, належного використання обладнання та засобів підприємства, а також гідні поваги правила поведінки, очікувані підприємством. Контрактори та користувачі третьої сторони можуть бути пов'язані з зовнішньою організацією, від якої можна у свою чергу вимагати вступу в контрактні угоди від імені контрактної особи.

Протягом найму повинні бути визначені відповідальність керівництва та гарантії, що на підприємстві організація безпеки здійснюється протягом всього найму особи.

Для мінімізації можливих ризиків безпеки всьому найманому персоналу, контракторам та користувачам третьої сторони повинен бути забезпечений відповідний рівень поінформованості, освіти та навчання щодо процедур безпеки та коректного використання засобів оброблення інформації. Повинен бути встановлений офіційно оформлений дисциплінарний процес обробки порушень безпеки.

Керівництво повинно вимагати від найманого персоналу, контракторів та користувачів третьої сторони застосування безпеки згідно з установленими на підприємстві правилами та процедурами.

Відповідальність керівництва повинно охоплювати забезпечення того, щоб найманий персонал, контрактори та користувачі третьої сторони були належним чином ознайомлені зі своїми ролями щодо інформаційної безпеки та відповідальність перед наданням доступу до чутливої інформації або інформаційних систем; забезпечені настановами для встановлення на підприємстві очікуваної безпеки їх ролей; мотивовані на виконання політики безпеки підприємства.

Мотивація на виконання політики безпеки охоплює: усвідомлення важливості дотримання процедур, інструкцій, настанов тощо, розуміння своєї відповідальності і наслідків невідповідних дій чи зловживань інформацією або засобами оброблення інформації на підприємстві до яких надано доступ, а також знання дисциплінарного процесу і впевненість, що своєчасні попередження про інциденти інформаційної безпеки чи власні ненавмисні

порушення безпеки і виконання передбачених для цих випадків дій призведе до менших втрат для підприємства та наслідків для особи, що їх спричинила [2].

Якщо найманий персонал, контрактори та користувачі третьої сторони не про інформовано щодо їх відповідальності стосовно безпеки, вони можуть спричинити значну шкоду підприємству. Мотивований персонал ймовірніше буде більш надійним і спричинятиме менше інцидентів інформаційної безпеки.

Незадовільне управління може викликати у персоналу недооцінення, що призводить до негативних впливів на безпеку підприємства. Наприклад, незадовільне управління може призвести до нехтування безпекою або потенційного зловживання активами підприємства.

Увесь найманий персонал підприємства, а там, де це суттєво, і контрактори та користувачі третьої сторони повинні отримувати належне навчання для про інформованості та регулярно отримувати оновлені дані щодо політик і процедур безпеки підприємства, суттєвих для їх посадових обов'язків.

Навчання для поінформованості повинно починатися з офіційно оформленої процедури, спроектованої для ознайомлення з політикою безпеки підприємства та очікуваннями до надання доступу до інформації або послуг.

Рекомендується започаткувати офіційну процедуру навчання правилам роботи на комп'ютерах, основам політики безпеки підприємства, правилам поведінки та поводження з організаціями-партнерами тощо для усіх категорій працівників підприємства.

Продовження навчання повинно охоплювати вимоги безпеки, правові відповідальності та бізнес-контролі, а також навчання коректному використанню засобів оброблення інформації, наприклад, процедурі реєстрації, використанню пакетів програмного забезпечення та інформації щодо дисциплінарного процесу.

Поінформованість з безпеки, освіта та навчання повинні бути суттєвими і відповідати ролі, відповідальності та навичкам особи, повинні охоплювати інформацію щодо відомих загроз, належних каналів звітування щодо інцидентів інформаційної безпеки і того, з ким контактувати для отримання подальших рекомендацій з безпеки.

Навчання для поліпшення поінформованості призначене для того, щоб надати можливість працівникам усвідомити проблеми та інциденти інформаційної безпеки і реагувати згідно з потребами їхніх посадових обов'язків.

Повинен існувати офіційно оформлений дисциплінарний процес щодо найманого персоналу, який здійснив порушення безпеки.

Дисциплінарний процес не повинен розпочинатися без попередньої верифікації того, що порушення безпеки сталося.

Офіційно оформлений дисциплінарний процес повинен забезпечувати коректний та справедливий розгляд справи найманого персоналу, якого підозрюють у вчиненні порушень безпеки. Повинен існувати офіційно оформлений дисциплінарний процес для диференційованого реагування, яке бере до уваги такі фактори: відповідне законодавство, бізнес контракти, сутність та тяжкість порушення і його вплив на бізнес, чи є це перше або повторне правопорушення, проходив чи ні порушник належне навчання, а також інші необхідні фактори. У серйозних випадках неналежного поводження процес повинен передбачати невідкладне позбавлення обов'язків, прав доступу та повноважень і негайне випроваджування, за необхідності, з місцеперебування.

Дисциплінарний процес повинен також використовуватися як фактор утримування від порушень політики та процедур безпеки, а також будь-яких інших порушень безпеки найманим персоналом, контакторами і користувачами третьої сторони.

Коли припиняються або змінюються умови найму, то повинно бути встановлені відповідальність та гарантії, що найманий персонал, контрактори та користувачі третьої сторони, коли покидають підприємство, то це відбувається під контролем служби безпеки підприємства, фіксується що робота завершена і все обладнання повернене, а також всі права доступу видалені. Для цього повинні бути чітко визначені та встановлені правила і відповідальність за виконання процедур припинення найму або зміни умов найму.

При припиненні найму повинно доводитися до відома вимоги безпеки, що продовжують діяти, та правова відповідальність, і, за необхідності, відповідальності, що містяться у будь-якій угоді щодо конфіденційності, які продовжуються на визначений період після звільнення найманого персоналу, контрактора або користувача третьої сторони.

Відповідальність та обов'язки, які ще чинні після припинення найму, повинні міститися у контрактах найманого персоналу, контрактора або користувача третьої сторони.

Зазвичай відділ кадрів є відповідальним за весь процес припинення найму і для управління аспектами безпеки суттєвих процедур співпрацює з безпосереднім керівником особи, що звільняється. У випадку, коли це контрактор, цей процес припинення відповідальності може виконувати організація яка відповідальна за контрактора, а у випадку іншого користувача це може виконувати його організація.

Увесь найманий персонал, контрактори та користувачі третьої сторони повинні повернути всі активи підприємства, що перебувають у їх володінні, після припинення їх найму, контракту чи угоди.

Офіційно оформлений процес припинення найму повинен включати повернення усього раніше виданого програмного забезпечення, корпоративних документів та обладнання. Також треба повернути інші активи підприємства, такі як мобільні обчислювальні пристрої, кредитні картки, картки доступу, програмне забезпечення, інструкції та інформацію, збережену на електронних носіях.

Якщо найманий персонал, контрактори та користувачі третьої сторони купують обладнання, що належить підприємству, або використовують своє власне персональне обладнання, треба слідувати процедурам, які забезпечують, що вся інформація що належить підприємству передається йому і надійно видаляється з обладнання.

У випадках, коли найманий персонал, контрактори та користувачі третьої сторони мають відомості, важливі для подальшого функціонування підприємства, ця інформація повинна бути задокументована і передана підприємству.

Після припинення найму, контракту чи угоди будь-якого найманого персоналу, контракторів і користувачів третьої сторони права їх доступу до інформації та засобів оброблення інформації повинні бути вилучені або пристосовані до зміни. Права доступу, які повинні бути видалені або адаптовані, стосуються фізичного та логічного доступу, ключів, ідентифікаційних карток, засобів оброблення інформації, передплати (підписки), видалення з будь-якої документації, яка ідентифікує його як наявного представника підприємства.

За деяких обставин права доступу можуть розподілятися таким чином, щоб бути доступними більшій кількості людей, ніж звільнюваний найманий персонал, контрактор або користувач третьої сторони, наприклад, групові ідентифікатори. За таких обставин особи яких звільняють повинні бути видалені з усіх списків групового доступу, і повинні бути вжиті заходи, щоб рекомендувати іншому найманому персоналу, контракторам або користувачам третьої сторони, яких це стосується, далі не використовувати інформацією спільно із особою яку звільняють.

У випадках припинення найму, ініційованого керівництвом, ображений найманий персонал, контрактор або користувач третьої сторони можуть навмисно зіпсувати інформацію або пошкодити засоби оброблення інформації. У випадку відставки людей вони можуть зробити спробу зібрати інформацію для майбутнього використання.

Висновки. Ретельна організація управління матеріальними ресурсами, а також підбір і управління персоналом для захисту інформаційної безпеки є ключовими для навігації у складних умовах сучасного бізнес-ландшафту. Застосовуючи комплексний підхід і узгоджуючи процеси, підприємства можуть підвищити операційну ефективність і захистити свої цифрові активи, забезпечуючи стійке та процвітаюче майбутнє.

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.