УДК 338.22

[https://doi.org/10.52058/2786-5274-2022-2\(4\)-251-257](https://doi.org/10.52058/2786-5274-2022-2(4)-251-257)

Тютченко Світлана Миколаївна кандидат економічних наук, доцент, доцент кафедри економічної та інформаційної безпеки, Дніпропетровський державний університет внутрішніх справ, пр. Гагаріна, 26, м. Дніпро, тел.: (050) 363-34-86, <https://orcid.org/0000-0001-8480-6519>

НАПРЯМКИ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Анотація. У сучасному світі інформаційна безпека підприємства відіграє майже головну роль та вимагає розробки та впровадження заходів щодо її захисту та збереження. В процесі обігу та використання корпоративної інформації виникають відносини, які повинні регулюватися правовими законами. За останні роки сформувався великий обсяг законодавчих актів, що регулюють інформаційну сферу, зокрема сферу інформаційної безпеки та захисту інформації. В статті досліджується проблема підвищення інформаційної безпеки підприємств, одним з напрямків якої є контроль службової електронної пошти персоналу підприємства. Для цього в статті проаналізовано правові зобов'язання підприємств щодо контролю службової пошти персоналу та право на повагу до приватного життя. Корпоративна електронна адреса повинна використовуватися лише для ділового листування. Роботодавець повинен гарантувати конфіденційність кореспонденції та права на повагу до приватного життя, але, одночасно і мати право захищати таємницю компанії, яку працівникам забороняється розголошувати.

Автором проаналізовано наукові праці в питанні правового забезпечення інформаційної безпеки підприємств та констатовано, що при контролі службової електронної пошти персоналу, роботодавець повинен керуватися принципом необхідності, захисту гідності та особистих прав персоналу, принципом свободи та незалежності.

В статті представлений моніторинг роботи персоналу та втручання в їхнє право на повагу до приватного життя. Використання положень Закону повинно здійснюватися з урахуванням необхідності збалансовувати ці суперечливі цінності та інтереси обох сторін трудових відносин. А це значить, що моніторинг, як вид контролю роботодавця повинен враховувати потребу поважати особисті права працівників, включаючи право на приватне життя.

Ключові слова: інформаційна безпека, електронна пошта, приватне життя, Європейський суд, право, Трудовий кодекс.

Tiutchenko Svitlana Mykolayivna PhD in Economics, Associate professor of the Department of Economic and Information Security Dnipropetrovsk State University of Internal Affairs, Gagarina Ave., 26, Dnipro, tel.: (050) 363-34-86, <https://orcid.org/0000-0001-8480-6519>

DIRECTIONS FOR IMPROVING ENTERPRISE INFORMATION SECURITY

Abstract. Nowadays, enterprise information security plays an almost major role and requires the development and implementation of measures to protect and preserve it. In the process of circulation and use of corporate information, the relationships that must be governed by legal laws appear. In recent years, a large number of legislative acts regulating the information sphere have been formed, in particular, the sphere of information security and information protection. The article researches the problem of improving the information enterprises' security, one of the areas of which is the control of business e-mail of enterprise personnel.

The article analyzes the legal obligations of enterprises to control the service mail of staff and the right to respect for private life. The corporate email address should only be used for business correspondence. The employer must guarantee the confidentiality of correspondence and the right to respect for private life, but at the same time have the right to protect the secrecy of the company, which employees are prohibited from disclosing.

The author analyzed the scientific work on the legal security of information security of enterprises and states that in controlling the official e-mail of staff, the employer must be guided by the principle of necessity, protection of dignity and personal rights of staff, the principle of freedom and independence.

The monitoring of staff work and interference in their right to respect for private life is presented in the article. The usage of the provisions of the Law should take into account the need to balance these conflicting values and interests of both parties to the employment relationship. This means that monitoring, as a form of employer control, must take into account the need to respect the personal rights of employees, including the right to privacy.

Keywords: information security, e-mail, private life, European Court, law, Labor Code.

Постановка проблеми. Актуальність вивчення різних аспектів інформаційної безпеки пов'язана із глобалізацією процесів, в яких постійно зростає значення інформації. Інформація виступає як важливий елемент для функціонування держави, демократичного розвитку суспільства, взаємовідносин між громадянами, державою та суспільством. Інформаційні права людини розглядаються як невід'ємна складова громадянських прав.

Тож перед керівниками та власниками виникає проблема забезпечення інформаційної безпеки підприємства. Кожен роботодавець повинен розробити

та впровадити комплекс заходів захисту інформації від несанкціонованого доступу, забезпечити її конфіденційність, доступність та цілісність.

Аналіз останніх досліджень і публікацій. Вивченням науково-теоретичних проблем інформаційної безпеки займалися вітчизняні вчені М.Т. Дзюба, М.І Іванова., М.І. Онищук, А.М. Ткаченко та багато інших. Але проблема щодо контролю службової електронної пошти як інструменту підвищення інформаційної безпеки підприємства досліджувалося частково.

Мета статті - дослідження питання контролю службової електронної пошти персоналу підприємства як одного з напрямків підвищення інформаційної безпеки.

Виклад основного матеріалу. Сучасні підприємства використовують Інтернет як основний інструмент для розвитку ділової активності та охоплення ринку, що призводить до високих економічних результатів. Поряд з цими перевагами з'являються різні загрози безпеки для конфіденційної важливої корпоративної інформації.

У сучасному світі інформаційна безпека підприємства відіграє майже головну роль та вимагає розробки та впровадження заходів щодо її захисту та збереження. Раніше безпека розглядалася як державна або політична функція, але стрімкий розвиток сучасних інформаційних технологій вимагає впровадження нових законів, положень та програм щодо захисту інформації, персональних даних та активів в межах підприємства [1].

В наш час стрімкого інформаційного та технологічного розвитку суспільства роботодавці все частіше стикаються з питанням ефективності та продуктивності роботи своїх працівників. Сьогодні кожен працівник на будь-якому підприємстві має службову електронну пошту - поштову скриньку, яка пов'язана з доменом підприємства та призначена для ідентифікації співробітників компанії в відносинах з іншими підприємцями. Ця електронна адреса може бути використана не тільки для того, щоб працівник виконував діяльність в рамках контракту з підприємством, але може бути застосована для інших цілей - приватних, що може привести до негативних наслідків для підприємства. Щоб уникнути ситуації, в якій працівник використовує службову електронну пошту у власних цілях, роботодавець повинен мати інструменти, які дозволяють йому перевірити, з якою метою працівник використовує службову електронну пошту. Це необхідно зробити так, щоб право на приватне життя і таємницю кореспонденції працівника не було порушено.

Відповідно до законодавства, роботодавець має право перевіряти кореспонденцію, що надсилають його працівники, які використовують службову електронну пошту. Працівники ведуть листування від імені роботодавця – тож цілком логічно, що роботодавець має право знати її зміст.

Контроль ділової електронної пошти можливий, але він повинен мати чітко визначену мету, яка полягає в підвищенні ефективності роботи

працівників та здатність перевіряти, чи використовують вони інструменти, надані їм роботодавцем за призначенням [2].

Неприпустимість відсутності правових підстав для перевірки електронної пошти працівника підтверджує досвід законодавства інших країн. Наприклад, Британський закон прямо передбачає винятки із заборони підслуховування роботодавцем телефонної розмови працівника та читання його електронних листів (без згоди відправника та одержувача повідомлення). Роботодавець має право контролювати та фіксувати повідомлення в певних обставинах, у тому числі для забезпечення того, щоб працівники відповідали стандартам підприємства, запобігали чи виявляли злочин, розслідували чи виявляли несанкціоноване використання телекомунікаційної системи або забезпечували безпеку системи або її ефективне функціонування. Фінський закон про захист конфіденційності в професійному житті регулює правила контролю роботодавцем електронної пошти працівника, а саме, відновлення та відкриття повідомлень, що надсилаються на електронну адресу працівника підприємства та повідомлення, надіслані працівником з цієї адреси [3].

Кодекс законів про працю «замовчує» питання можливості роботодавця контролювати виконання працівниками своїх трудових обов'язків. Є лише загальні положення, виходячи з яких можемо стверджувати, що працівник має бути попереджений про здійснення роботодавцем контролю.

Враховуючи практику ЄСПЛ, можна стверджувати, що перевірка електронної переписки та, здійснення контролю роботодавцем за роботою працівника є умовою праці, про яку працівник, має бути заздалегідь попереджений. Відповідно до ст. 29 Кодексу законів про працю України при прийомі працівника на роботу, до початку виконання трудових обов'язків він має бути повідомлений під розписку про умови праці, в тому числі й про можливість та порядок використання працівником технічних засобів, що містяться на робочому місці, для особистих потреб та в особистих цілях. У випадку ж, коли роботодавець вирішив запровадити контроль вже в період роботи працівника, працівника слід, відповідно до ст. 32 Кодексу законів про працю, не пізніше ніж за два місяці до запровадження контролю попередити про зміни в організації праці, а саме: щодо запровадження контролю за роботою працівника та можливої перевірки роботодавцем електронної переписки, користування Інтернетом, перевірки телефонних дзвінків чи здійснення відеозапису. Якщо працівник не згоден із такими нововведеннями роботодавця, трудовий договір з ним може бути припинений на підставі п. 6 ст. 36 Кодексу законів про працю [4].

Отже, моніторинг офіційної електронної пошти працівника є допустимим, якщо це необхідно для забезпечення належної організації роботи та належного використання інструментів праці, наданих працівникові.

При контролі службової електронної пошти працівника, роботодавець повинен керуватися такими принципами:

- а) принцип необхідності;
- б) принцип захисту гідності та особистих прав працівника;
- в) принцип свободи та незалежності.

Згідно з принципом необхідності, моніторинг електронної пошти працівника допустимий, коли це необхідно для забезпечення такої організації роботи, що дозволяє в повній мірі використовувати робочий час і робочі інструменти, доступні співробітникам. Під критерієм необхідності слід розуміти те, що роботодавець зобов'язаний вказати, що вищезазначені цілі не можуть бути досягнуті інакше, як лише шляхом обраної форми моніторингу працівників.

Працівник повинен бути повідомлений про моніторинг роботодавцем його службової електронної пошти. Працівник, який не був проінформований роботодавцем про моніторинг службової пошти, має законні підстави сподіватися, що його приватне життя і комунікація захищені [2].

При введенні такої форми контролю, роботодавець зобов'язаний інформувати працівників за 2 тижні до початку перевірки. При прийнятті на роботу нового працівника підприємство повинно надати йому письмову інформацію про цілі, обсяги та способи моніторингу пошти, перш ніж дозволити йому виконувати обов'язки. Крім того, роботодавець повинен ввести відповідні позначення на поштових скриньках працівників, чітко вказуючи, що електронна пошта контролюється підприємством [5].

Цілі, обсяг та спосіб застосування вищезазначеної форми моніторингу повинні бути вказані в колективному трудовому договорі чи нормативно-правових актах. Роботодавець повинен визначити цілі моніторингу, точно вказавши обсяг здійснення контрольної діяльності. Необхідно визначити масштаб моніторингу та те, які дані будуть збиратися в результаті його використання. Обсяг даних повинен відповідати цілям моніторингу. Тому, якщо достатньо отримати інформацію про відправників та одержувачів зв'язку, а також дату та час надсилання та отримання повідомлень, а також тему повідомлення, підприємство не повинно аналізувати зміст кореспонденції. Предметом домовленостей також повинен бути спосіб використання моніторингу, а отже, визначення засобів здійснення контролю електронної пошти та правил їх використання. Зокрема, слід визначати обставини та періодичність проведення контролю [5].

Відповідно до Трудового кодексу моніторинг електронної пошти не може порушувати таємницю кореспонденції і право на приватність життя.

Безперечно, право працівників до таємниці кореспонденції може бути порушеним внаслідок використання електронної пошти для моніторингу. Хоча право дозволяє контролювати лише службові повідомлення, існує ризик навіть випадково знайти приватні повідомлення в службовій поштовій скриньці працівника.

Як підкреслюється в дослідженнях, навіть якщо роботодавець забороняє використовувати службову пошту в приватних цілях і настановується на

приватну кореспонденцію працівника, який не виконав цієї заборони, він не може прочитати її повністю. Порухення таємниці листування може навіть призвести до кримінальної відповідальності, а також до порушення Конвенції про захист прав людини і основоположних свобод.

Щоб уникнути ненавмисного порушення приватного простору працівника, пропонується ввести відповідні визначення приватних повідомлень працівника. Але, найпростішим способом для роботодавця є заборона використовувати офіційну пошту в приватних цілях [6].

Висновки. Кожен роботодавець зацікавлений у високопродуктивній роботі працівника та його свідомому ставленні до своїх обов'язків. Тож роботодавець повинен мати можливості правомірно контролювати виконання працівниками їх трудових обов'язків на робочому місці та дотримання ними вимог конфіденційності щодо інформації, документів та будь-яких інших даних, визначених роботодавцем як конфіденційні. Працівники повинні бути попереджені про те, яких заходів вживатиме роботодавець для забезпечення інформаційної безпеки у функціонуванні підприємства.

Література:

1. Тютченко С.М., Бут К. А. Інформаційна безпека на підприємстві. *Економічна та інформаційна безпека: актуальні питання та інновації. Матеріали міжнар. наук.-практ. конф.* 4 листоп. 2021 р. Дніпро. Дніпроп. держ. ун-т внутр. справ. 2021. с. 235.
2. Яськовський К. Трудовий кодекс Республіки Польща. Коментар. Польща. URL: <https://sip.lex.pl/#/commentary/587787380/584820>
3. Закон про захист приватності у трудовому житті. Act on the Protection of Privacy in Working Life (759/2004). URL: <https://www-dataguidance-com.translate.goog/legal-research/act-protection-privacy-working-life>
4. Як правомірно здійснювати контроль за виконанням працівниками трудових обов'язків. URL: <http://kmp.ua/uk/analytics/exclusive/how-to-control-the-employees-observance-of-job-duties-lawfully/#>
5. Рибальченко Л. В., Рижков Е. В., Тютченко С. М. та ін. Безпека підприємництва. Монографія. Дніпро. Видавець Біла К. О. 2020. 180 с.
6. Рішення Європейського Суду з прав людини від 25 червня 1997 року, Заява № 20605/92, в справі Гелфорд проти Сполученого Королівства. URL: http://kryminologia.ipsir.uw.edu.pl/images/stronka/ETPCz/A.%20Rzeplinski_Wyrok%20ETPCz_Sprawa%20Halford%20przeciwko%20Zjednoczonemu%20Krolestwu.pdf

References:

1. Tyutchenko, S.M., But, K. A. (2021). Informaciina bezpeka na pidpriemstvi. [Information security at the enterprise]. *Ekonomichna ta informaciina bezpeka: aktualni pitannya ta innovacii. Materiali mijnar. nauk. _prakt. konf. Dnipro.(pp.235-236). Dniprop. derj. un_t vnutr. Sprav* [in Ukrainian].
2. Yaskovskii K. Trudovii kodeks Respubliki Polska. Komentar. Polska. [Labor Code of the Republic of Poland. Comment. Poland]. (n.d.). *LEX.pl*. Retrieved from <https://sip.lex.pl/#/commentary/587787380/584820>
3. Zakon pro zahist privatnosti u trudovomu jitti. [Act on the Protection of Privacy in Working Life (759/2004)]. (n.d.). *zakon.rada.gov.ua*. Retrieved from <https://www-dataguidance-com.translate.goog/legal-research/act-protection-privacy-working-life> [in Ukrainian]

4. Yak pravomirno zdiisnyuvati kontrol za vikonannyam pracivnikami trudovih obov'yazkiv. [How to legally monitor the performance of employees' duties]. (n.d.). *khpg.org*. Retrieved from http://kmp.ua/uk/analytics/exclusive/how_to_control_the_employees_observance_of_job_duties_lawfully/# [in Ukrainian]

5. Ribalchenko, L. V., Rijkov, E. V., Tyutchenko, S. M. ta in. (2020). *Bezpeka pidpriemnictva*. [Business security]. Dnipro: Vidavec Bila K. O. [in Ukrainian].

6. Rishennya Європейського Суду з прав людини від 25 червня 1997 року_ Заява № 20605/92_ в справі Gelford проти Spoluchenogo Korolivstva. [Judgment of the European Court of Human Rights of 25 June 1997, Application № 20605/92, in the case of Gelford v. The United Kingdom]. (n.d.). *khpg.org*. Retrieved from http://kryminologia.ipsir.uw.edu.pl/images/stronka/ETPCz/A.%20Rzeplinski_Wyrok%20ETPCz_Sprawa%20Halford%20przeciwko%20Zjednoczonemu%20Krolestwu.pdf