**DOI 10.36074/logos-31.03.2023.10**

# ЗАХОДИ КОРПОРАТИВНОЇ БЕЗПЕКИ ПІД ЧАС ВІДДАЛЕНОЇ РОБОТИ ЗІ КОНФІДЕНЦІЙНИМИ ДАНИМИ

**Жалай Любов Сергіївна**
студентка 4 курсу освітньої програми «Документаційне забезпечення управління та інформаційно-аналітична діяльність»
*Волинський національний університет імені Лесі Українки*

**Чибирак Світлана Вікторівна**
канд. іст. наук, доцент кафедри музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності
*Волинський національний університет імені Лесі Українки*

*УКРАЇНА*

Безпека є комплексним засобом із захисту інтересів комерційних установ. Вона включає в себе три основні рівні: люди, технології та процеси. І людина є найслабшою ланкою у цій системі [2]. Безпека повинна бути тісно пов'язана з кожним процесом і врахована у кожному управлінському рішенні, особливо якщо мова йде про перехід до віддаленої зайнятості, який супроводжується певними загрозами. Безпека установи не є виключно роботою департаменту, що спеціалізується у цьому питанні, це відповідальність кожного співробітника. Саме тому роботодавець і співробітник увагу мають приділяти питанням захисту своєї діяльності, особливо комерційних і конфіденційних даних.

Насамперед, активна підготовка працівників до будь-якої з форм безпечної віддаленої роботи, зі сторони роботодавця, здійснюється за допомогою застосування кількох стратегічних заходів, включаючи: укладення додаткових угод про нерозголошення комерційної таємниці та конфіденційної інформації установи; регулювання віддаленої зайнятості в установі внутрішніми організаційними документами; навчання працівників інформаційній, цифровій та медіа грамотності. Окрім того, з працівниками, які хочуть перейти на віддалену форму зайнятості, але не мають відповідного технічного забезпечення, укладається додатковий договір про надання відповідного обладнання для відділеної співпраці. Зауважимо, що технічне обладнання, надане в користування віддаленим працівникам, має мати програмне забезпечення для захисту від загроз втрати конфіденційної інформації.

Коли мова йде про заходи, які здійснюватимуться зі сторони віддаленого працівника, який використовуватиме власне технічне забезпечення, то вимоги до організації віддаленого робочого місця відрізняються. Роботодавець повинен провести навчання працівників щодо самостійного встановлення ними аналогічних заходів захисту та перевірити виконання цих умов.

Важливим моментом віддаленої зайнятості працівників комерційних структур є робота з комерційною таємницею та конфіденційної інформацією, адже поза межами фактичного місця роботи існує фізична можливість доступу до неї сторонніх осіб. Найбільшого захисту потребує інформація, що стосується продуктів та даних клієнтів. Зі зрозумілих причин, етапи її захищеності в кожній компанії різні та не розголошуються. Друга за захистом – внутрішня інформація, що включає й особисту кореспонденцію.

Якщо працівник використовує в роботі конфіденційні дані або інформацію, яка становить комерційну таємницю, що охороняється законом, він підписує спеціальну угоду про нерозголошення відомостей або до його договору про будь-який із видів віддаленої діяльності включаються умови, згідно з якими на нього покладається обов'язок збереження такої таємниці, зокрема і через використання спеціальних засобів її захисту. Якщо ж усе одно трапився витік інформації зі сторони працівника, – він зобов'язаний негайно повідомити про це роботодавця для усунення наслідків, що можуть бути спричинені втратою даних, та запобігання подальшого витоку інформації [1].

Пропонуємо вжиття наступних системних заходів за допомогою кооперації учасників трудових відносин. Зі сторони роботодавця варто: 1) надати працівникам необхідного обладнання, програмно-технічних засобів, засобів захисту інформації та іншого устаткування; 2) організувати навчання віддалених працівників щодо самостійного встановлення ними аналогічних засобів захисту власного обладнання, яке не знаходиться під контролем роботодавця; 3) перевіри наявність сертифікатів безпеки кожного пристрою, наданого для віддаленої роботи; 4) забезпечити віддалених співробітників надійним хмарним сховищем для зберігання та обробки даних, встановивши контроль та розмежувавши доступ до інформації відповідно до повноважень працівників; 5) запобігати неналежному використанню службового часу або ресурсів; 6) передбачити незалежні від зовнішніх умов канали зв'язку. Зі сторони віддалених працівників необхідно: 1) організувати віддалене робоче місце таким чином, щоб унеможливити доступ сторонніх осіб до конфіденційної та комерційної інформації; 2) здійснювати вхід та використовувати у наданих для роботи чи особистих пристроях не персональний, а корпоративний обліковий запис, електронну пошту тощо; 3) застосовувати стійкі паролі до пристроїв, систем та платформ, регулярно їх змінювати та нікому не передавати; 4) налаштувати багатофакторну автентифікацію; 5) установити додаткові плагіни безпеки та антивіруси; 6) вимкнути на робочих пристроях функцію автоматичного підключення до незахищених мереж; 7) під час візуалізації даних (наприклад при демонстрації екрану) виходити із корпоративних чатів, що дозволить уникнути випадкового поширення інформації; 8) слідкувати за оновленнями програм; 9) повідомити роботодавця у разі, якщо виникла загроза витоку інформації.

Отож, впроваджуючи віддалену роботу, роботодавцеві досить складно забезпечити належне функціонування системи корпоративної безпеки, що пов'язано зі зменшенням інструментів контролю за віддаленими працівниками та використанням корпоративних інформаційних ресурсів у незахищених мережах (на противагу локальним мережам). З метою запобігання можливих та боротьби з реальними загрозами в зазначеному напрямі, пропонуємо послуговуватись послідовністю запропонованих у дослідженні заходів, що сприятимуть створенню ефективної системи корпоративної безпеки.

## Список використаних джерел:

[1] Луняк, М. (2021). Трудове законодавство для віддалених працівників – норми, які могли б стати ефективними : веб-сайт Freelancehunt. Вилучено з: https://cutt.ly/sMOJlFn.

[2] Основи кібергігієни : освітній серіал на платформі Дія. Цифрова освіта. Вилучено з: https://cutt.ly/a821Y1B.