

5. Прокопенко В.І. Трудове право України / В.І. Прокопенко. [Електронний ресурс]. – Доступний з <http://uasol.com/index.php?aid=574>.

6. Ветлужских Е. Мотивация и оплата труда. Инструменты. Методики. Практика / Е. Ветлужских. – М. : Изд-во "Альпина Бизнес Букс", 2007. – 133 с.

7. Фещур Р.В. Статистика теоретичні засади і прикладні аспекти : навч. посібн. / Р.В. Фещур, А.Ф. Барвінський, В.П. Кічор. – Львів : Вид-во "Інтелект-Захід", 2003. – 576 с.

8. Саєнко М.Г. Стратегія підприємства в умовах ринкових відносин : навч. посібн. – Вид. 2-ге, [перероб. і доп.] / М.Г. Саєнко, П.С. Смоленюк, З.Ф. Бриндзя, Л.М. Маланчук. – Хмельницький : Вид-во "Наук. думка". – 2009. – 215 с.

Вороновская М.М. Применение системы премирования по обобщенным грейдам для стимулирования инновационной деятельности предприятий

Исследована инновационную деятельность предприятий, отмечено значение стимулирования инновационной деятельности в обеспечении ее развития, рассмотрены премиальные системы предприятия. Для стимулирования инновационной деятельности предприятия обосновано применение системы премирования за обобщенными грейдами, рекомендована последовательность формирования такой системы.

Ключевые слова: инновационная деятельность, мотивирование, стимулирование, премиальные системы, обобщенный грейд.

Voronovska M.M. Application of bonus generalized grade system is for stimulation of innovative activity of enterprises

Investigational innovative activity of enterprises, underline value of stimulation of innovative activity in providing of its development, the bonus systems of enterprise are considered. For stimulation of innovative activity of enterprise grounded application of the bonus grade system, the sequence of its forming is made to order

Keywords: innovative activity, reason, stimulation, bonus systems, generalized grade.

УДК 658.6:658.34

Ст. викл. Н.М. Галла¹ – Донецький НУ економіки і торгівлі ім. Михайла Туган-Барановського

ВИТІК КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ – ВНУТРІШНЯ ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ ТУРИСТИЧНОГО ПІДПРИЄМСТВА

Розглянуто сутність та обґрунтування необхідності захисту комерційної інформації в туристичному підприємстві. Описано засоби контролю співробітників, які мають доступ до бази даних підприємства. Запропоновано шляхи вирішення проблем витоку конфіденційної інформації та контролю використання робочого часу на підприємстві.

Ключові слова: конференційна інформація, внутрішні загрози економічній безпеці, контроль робочої години, витік інформації, інсайдери.

Постановка проблеми. В умовах сучасного бізнесу, перед будь-якою організацією, що працює з персональними даними, має свій список клієнтів або, що займається розробленнями в різних галузях, рано чи пізно стає питання захисту важливих даних, виявлення й запобігання витоків інформації. Туристичне підприємство не є винятком.

¹ Наук. керівник: проф. О.В. Виноградова, д-р екон. наук – академік академії економічних наук України

Не секрет, що головною цінністю для будь-якого підприємства туристичного бізнесу є напрацьована роками клієнтська база, яка найчастіше зберігається в цифровому форматі й належить до об'єктів комерційної таємниці.

Аналіз останніх досліджень і публікацій. Дослідженню проблем забезпечення комерційної таємниці приділено увагу в роботах вітчизняних науковців та зарубіжних дослідників, таких як: Т. Гладченко, В. Забродський, Н. Капустін, С. Лихова, В. Попович, В. Шликов та ін. Питання, пов'язані з використанням робочого часу на підприємстві, досліджували такі вчені, як: В. Гупалов, Н. Вишневецька, Л. Лутай та ін. Водночас питання забезпечення належного рівня безпеки конфіденційної інформації та раціонального використання робочого часу в туристичному підприємстві ще мало вивчене і потребує великої уваги.

Мета дослідження. Розкрити специфіку захисту комерційної інформації й контролю використання робочого часу в туристичному підприємстві.

Виклад основного матеріалу. Для визначення сутності конфіденційної інформації необхідно зазначити, що це поняття входить до більш широкого поняття – "Комерційна таємниця".

Поняття комерційної таємниці надане в ст. 30 Закону України від 27.03.91 "Про підприємства в Україні": "Під комерційною таємницею підприємства мають на увазі відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам".

Стаття 1 цього Закону визначає: "Підприємництво – самостійний господарюючий статутний суб'єкт, який має права юридичної особи та здійснює виробничу, науково-дослідницьку і комерційну діяльність з метою одержання відповідного прибутку (доходу)".

Виходячи з наведеного визначення, до підприємств у цьому розумінні можна віднести і туристичні підприємства [1].

Відповідно до ст. 30 Закону України "Про інформацію", конфіденційна інформація за своїм правовим режимом належить до інформації з обмеженим доступом. Її становлять "...відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов" [2].

Як бачимо, Закон не дає визначення інформації, що становить комерційну таємницю чи є конфіденційною, а замість цього надає необмежені права її власникам у частині встановлення переліку відповідних відомостей.

У зв'язку з цим розглянемо, які відомості належать до числа таких, що становлять комерційну і конфіденційну таємницю (за змістом наведених нами статей Закону "Про підприємства в Україні" і Закону "Про інформацію"), на практиці відносять до таких у туристичних підприємствах.

Відомості, що становлять комерційну таємницю:

1. Відомості про принципи управління туристичним підприємством:

- про підготовку, прийняття і виконання окремих рішень керівництва з усіх перелічених питань;
- про перспективні плани і методи управління туристичним підприємством;

- про факти підготовки, мету і проведення ділових переговорів, про предмет і цілі нарад, засідань;
 - документація управління,
 - відомості і документи, що стосується питань ділової політики туристичного підприємства.
2. Відомості про фінансову діяльність туристичного підприємства:
- ті, що розкривають планові і фактичні показники фінансового плану;
 - бюджет туристичного підприємства;
 - майновий стан туристичного підприємства;
 - про рівень прибутку туристичного підприємства;
 - про специфіку міжнародних розрахунків з іншими туристичними підприємствами;
 - про джерела кредитних ресурсів туристичного підприємства;
 - про стратегію і тактику з валютних і кредитних питань;
 - про методи розрахунків, структуру і величину знижок;
 - про умови за договорами (контрактами);
 - матеріали аудиторських перевірок і ревізій;
 - про порядок користування печаткою і штампами туристичного підприємства;
3. Відомості у сфері програмного забезпечення туристичного підприємства:
- комп'ютерні програми, що використовують у роботі туристичного підприємства;
 - ті дані, що зберігаються на магнітних носіях;
 - про паролі і коди, які використовують допущені до цієї роботи службовці туристичного підприємства під час входження у внутрішні комп'ютерні мережі.
4. Відомості про клієнтів і партнерів туристичного підприємства:
- систематизовані відомості про клієнтів туристичного підприємства і його контрагентів за договорами;
 - про відносини туристичного підприємства з іноземними партнерами.
5. Інші відомості:
- про порядок і стан організації захисту комерційної таємниці і конфіденційної інформації;
 - про порядок і стан організації охорони і пропускну режиму, систему сигналізації;
 - ті, що становлять комерційну таємницю чи конфіденційну інформацію клієнтів і контрагентів;
 - інформація служби безпеки туристичного підприємства, якщо така існує.

Перелік відомостей, що належать до конфіденційних

1. Відомості про персонал туристичного підприємства: ті, що знаходяться в особових справах службовців; про заплановані зміни в кадровій політиці; про чисельність і склад службовців, про фонд їх заробітної плати, а також про наявність вакантних робочих місць.
2. Відомості про систему матеріально-технічного забезпечення туристичного підприємства: про транспортні й енергетичні потреби; про маршрути і цілі поїздок; про розміщення підсобних приміщень, режим надходження цінностей, устаткування тощо, а також про систему їх охорони.

Крім зовнішніх загроз, таких як хакерські, рейдерські атаки, в туристичному підприємстві існують ще і внутрішні погрози з боку інсайдерів, тобто

співробітників компанії, які зі злим наміром або через незнання передають третій стороні інформацію, що становить комерційну таємницю. Саме внутрішні загрози становлять найбільшу небезпеку для економічної діяльності туристичного підприємства, тому що, по-перше інсайдери діють зсередини і, зазвичай, не обмежені в часі, а по-друге, потенційно, інсайдером може бути будь-який співробітник організації. Так, за даними щорічного огляду комп'ютерних злочинів "E-crime Watch Survey", у питаннях крадіжки інтелектуальної власності й персональних даних інсайдери помітно лідирують перед зовнішніми злочинцями.

Інсайдерів, що діють із корисливих спонукань, досить легко собі уявити, це можуть бути, наприклад, менеджер із продажу турів, який "зливає" дані на сторону. Витік інформації може відбутися й з необережності – наприклад, у разі втрати співробітником флеш-пам'яті із клієнтською базою, або під час налагодження системного блоку комп'ютера в сервісному центрі.

Згідно з даними останніх досліджень, найбільш "популярними" є такі канали витоку інформації: переносні запам'ятовувальні пристрої; електронна пошта; інтернет (web-пошта, форуми); інтернет-пейджери (ICQ, mail.ru agent, Skype тощо).

Як наслідок зі сказаного вище, значна частина каналів витоків так чи інакше пов'язана з Інтернет. Специфіка роботи туристичних компаній не дає змоги повністю відмовитися від мережі Інтернет, а, зокрема, використання програм обміну миттєвими повідомленнями, таких як ICQ, Skype тощо. Питання навіть не в технічній можливості заборони, а в тому, що ці засоби дуже часто необхідні для роботи. Через ICQ та електронну пошту менеджери із продажу турів бронюють авіаквитки, місця в готелях, спілкуються із клієнтами й партнерами, а на форумах – вивчають відгуки про курорти, готелі або ж дізнаються про політичну ситуацію в країні перебування клієнтів. Проте вихід із цієї ситуації знайти можливо за допомогою спеціалізованих програм, таких як: Lanagent, Workvisor, Staffcop тощо. Завдяки такому програмному забезпеченню можна не тільки контролювати інформаційні потоки, але й одержувати детальну картину робочого дня співробітників.

Серед основних можливостей програм подібного роду варто зазначити:

- визначення фактів підключення знімних USB – носіїв інформації, і можливість "тіньової копії" копійованих на них файлів;
- перехоплення повідомлень Інтернет-пейджерів, таких як ICQ, mail.ru agent, MSN, Skype тощо;
- перехоплення поштових повідомлень, як відправлених і отриманих через поштових клієнтів, так і відправлених через WEB-пошту (при цьому зберігаються й прикріплені до листів файли);
- контроль відвідуваних користувачами WEB-сайтів, файлів, що викладаються в Інтернет з можливістю заборони відвідування певних посилань і передачі певних типів файлів;
- запам'ятовування всіх текстів, що набираються на клавіатурі й копійованих у буфер-обміні;
- логування запуску й закриття програм, а також можливість заблокувати їхній запуск;

- виконання знімків екранів моніторів користувачів (скріншотів) за командою або через заданий проміжок часу;
- облік документів, відправлених до друку;
- оповіщення про виявлені порушення політики безпеки.

Інтерфейс даних програм простий і зручний у використанні, розгортання комплексу в мережі підприємства проводиться швидко й непомітно для підконтрольних співробітників.

Ще однією з найбільших загроз економічній безпеці туристичного підприємства є нераціональне використання робочого часу співробітників. Ні для кого не є секретом, що крім основної діяльності, більшість працівників туристичних фірм протягом робочого дня також устигають займатися своїми особистими справами, використовуючи офісну техніку. У низці випадків це припустимо, оскільки дійсно неможливо безвідривно працювати всі 8 годин поспіль, а після невеликої перерви продуктивність праці, зазвичай, підвищується. Однак, на жаль, трапляються й протилежні ситуації, коли співробітники роблять невеликі перерви в розвагах, щоб трохи попрацювати. По суті, цим самим вони обкрадають свого роботодавця як прямо, так і побічно. Прямо – за рахунок використання безкорисного, а іноді й небезпечного для підприємства Інтернет-трафіка (соціальні мережі, розважальні й порнографічні сайти). Побічно – за рахунок втраченої вигоди: через не виконані вчасно завдання, недоробку необхідних документів і т. ін. Особливо часто така тенденція спостерігається за відсутності керівника, наприклад, коли він у відрядженні. Крім того, контролювати особисто дії кожного працівника в організації, особливо там, де працює понад 10 осіб, – складне й найчастіше нездійсненне завдання.

На вирішення обох позначених вище завдань – контролю робочого часу й організації інформаційної безпеки, розроблено низку програм для ПК, які дають змогу контролювати діяльність співробітників підприємства, що працюють за комп'ютером, а також вести статистику використання комп'ютерного часу. Ведення логу програм, що запускаються, відстеження змісту буфера обміну, а також з'єднань із Інтернет та відвідуваних сайтів, дає змогу виявляти діяльність користувачів, що не має стосунку до роботи, а також ті дії, які можуть бути небезпечними для підприємства (копіювання важливих файлів, встановлення шкідливих програм). Знімки екранів комп'ютерів (скріншоти) уможливають візуальний контроль.

Зазвичай, важливою особливістю програм для контролю робочого часу є розширена система звітів, що дає змогу не тільки представити всю інформацію в зручному для ревізора вигляді, але й створити аналітичні звіти, що обчислюються, містять узагальнені статистичні дані з найважливіших показників: загальний час роботи й час простою комп'ютерної техніки, час роботи користувача в конкретній програмі, кількість відвідувань кожного web-сайту і т. ін. Вся отримана в такий спосіб інформація зберігається централізовано в базі даних, існує можливість автоматичного отримання статистики від контрольованих комп'ютерів, інформація передається по мережі в зашифрованому виді.

Проаналізувавши наведені засоби економічного убезпечення, можна зробити такі **висновки**:

1. Основними загрозами витоку конфіденційної інформації на підприємстві туристичного бізнесу є внутрішні джерела. Зазвичай, це співробітники

цього підприємства, що мають справу безпосередньо з інформацією у цифровому форматі.

2. Нераціональне використання співробітниками робочого часу приводить до зниження ефективності роботи підприємства. Контроль над використанням робочого часу є основним завданням керівника.
3. Проблема витоків інформації й контролю робочого часу можливо розв'язати за допомогою спеціалізованого програмного забезпечення, завдяки якому той, хто займається перевіркою, одержує комплексну картину дій користувачів на робочім місці. Такий спосіб захисту допоможе виявити співробітників, котрі як навмисне виносять за межі підприємства важливу інформацію, так і розголошують її з необережності.

Література

1. **Закон України** від 27.03.91 "Про підприємства в Україні". [Електронний ресурс]. – Доступний з <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=887-12>
2. **Закон України** від 13.10.2010 "Про інформацію". [Електронний ресурс]. – Доступний з <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12>
3. **Забродский В.** Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15-16. – С. 35-37. – С. 35.
4. **Попович В.М.** Економіко-кримінологічна теорія детінізації економіки : монографія / В.М. Попович. – Ірпінь : Академія державної податкової служби України, 2001. – 236 с.
5. **Носік Ю.В.** Права на комерційну таємницю в Україні : монографія / Ю.В. Носік. – К. : Вид-во КНТ, 2007. – 240 с.
6. **Карчевський В.М.** Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж : монографія / за наук. ред. Л.М. Кривоченко. – Луганськ : Луг. акад. внутр. справ ім. 10-річчя незалежності України, 2002. – С. 56.
7. **Лутай Л.А.** Дисципліна відносин: стратегія розвитку та механізм забезпечення : монографія / Л.А. Лутай. – Донецьк : ДонНУЕТ ім. М. Тугай-Барановського, 2007. – 377 с.
8. **Гупалов В.К.** Управление рабочим временем / В.К. Гупалов. – М. : Изд-во "Финансы и статистика", 1998. – 240 с.
9. **Вишневская Н.Т.** Динамика рабочего времени: сравнительный анализ / Н.Т. Вишневская // Мировая экономика и международные отношения. – 2001. – № 2. – С. 61-72.

Галла Н.М. Утечка конфиденциальной информации – внутренняя угроза экономической безопасности туристического предприятия

Рассмотрены сущность и обоснование необходимости защиты коммерческой информации в туристическом предприятии. Описаны средства контроля сотрудников, имеющих доступ к базе данных предприятия. Предложены пути решения проблем утечки конфиденциальной информации и контроля использования рабочего времени на предприятии.

Ключевые слова: конфиденциальная информация, внутренние угрозы экономической безопасности, контроль рабочего часа, утечка информации, инсайдеры.

Galla N.M. Leak of Confidential Information is an Internal Threats to Safety of Tourist Enterprises

The article reviews the nature and justification for the protection of commercial information in the travel business. The means of control employees who have access to a database company. The ways of solving problems of leakage of confidential information and control of working time in the company.

Keywords: confidential information, internal threats to economic security, control of working hours, the leaked information, insiders.