**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**Дніпропетровський державний університет
внутрішніх справ**

Кафедра економічної та інформаційної безпеки

**КОНСПЕКТ ЛЕКЦІЙ**

**з дисципліни «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА»**

Для здобувачів вищої освіти юридичного факультету,

спеціальності 262 "Правоохоронна діяльність"

що навчаються на бакалаврському рівні вищої освіти

**Дніпро – 2020**

Укладач: Гавриш О.С, старший викладач кафедра економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ.

Конспект лекцій обговорений та схвалений на засіданні кафедри економічної та інформаційної безпеки 26.08.2020р., протокол

№ 1

**ТЕМА 1. ОСНОВИ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ**

**ПЛАН ЛЕКЦІЇ:**

1. Сучасні особливості інформаційного розвитку

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

Конституція України від 28.06.1996 № 254к/95-ВР (Редакція від 21.02.2019).

Закони:

* Закон України «Про інформацію» від 02.10.1992 № 2657-XII
* Закон України «Про захист інформації в інформаційно-телекомунікаційних
* системах» від 05.07.1994 № 80/94-ВР
* Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
* Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Нормативні документи:

* НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
* Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
* НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
* НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
* НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

**Навчальні посібники, інші дидактичні та методичні матеріали:**

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем.–М.: ГТУим. Н.Э. Баумана, 2016.–252с.

2. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. –К.: ДУІКТ, 2016.–126с.

3. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.

4. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак;під ред. В.О. Хорошко.–Луганськ: Ноулідж, 2012.–480 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

**МЕТА ЛЕКЦІЇ:**

Вивчити сучасні особливості інформаційного розвитку, структуру процесу організації інформаційної безпеки суб’єкта підприємництва.

**ВСТУП**

Сучасні особливості інформаційного розвитку суттєво відбились на всі сфери суспільного життя в т. ч. і на підприємницькій діяльності. Формування, в результаті такого розвитку, інформаційних відносин є постійним атрибутом не лише діяльності, а і взагалі існування суспільства, громади, організацій, суб’єктів економічної діяльності. Така ситуація зумовила як певний прогрес, так і створила передумови до появи нового виду ризиків, небезпек та загроз – інформаційних.

1. **Сучасні особливості інформаційного розвитку**

У процесі взаємовідносин суб’єктів підприємництва інтенсивність інформаційних ризиків, небезпек та загроз характеризується якістю самих взаємовідносин. Якщо в умовах інформаційного співробітництва та взаємодії можливість їх виникнення є мінімальною, то у інших видах взаємовідносин підстави виникнення інформаційних ризиків, небезпек та загроз будуть суттєво зростати. У такому випадку суб’єкти підприємництва мають бути готовими вживати адекватні заходи захисту та протидії таким ризикам, небезпекам та загрозам. Безумовно, що захист та протидія зазначеним небезпекам та загрозам, мінімізація інформаційних ризиків в діяльності суб’єктів підприємництва мають формувати окремий напрямок забезпечення їх безпеки – інформаційну безпеку.

Сучасні уявлення про безпеку бізнесу взагалі і інформаційну зокрема є досить різноманітними, єдине бачення суті та змісту інформаційної безпеки відсутнє. Не вдаючись до детального аналізу точок зору різних авторів щодо розуміння інформаційної безпеки підприємництва, можна бачити наявність в них певних засад, якими автори ідентифікують інформаційну безпеку. Такими засадами виступає захист інформації. Якраз захист інформації є притаманним позиції переважної більшості авторів у їх розумінні суті інформаційної безпеки. Віддаючи належне таким міркуванням слід звернути увагу на багатофункціональність інформації, яка проявляється у підприємницькій діяльності. Як уже говорилося вище, інформація є основою знань, тобто інтелектуального потенціалу суб’єктів підприємництва і які безумовно необхідно захищати. В той же час інформація є умовою ефективного здійснення підприємницької діяльності, вона використовується як засіб впливу на ринкову ситуацію, взаємовідносини суб’єктів, інформація має комерційну цінність і може виступати окремим видом економічної діяльності. Тобто, відтотоження інформаційної безпеки лише з захистом інформації при такій різноманітності її властивостей і функцій буде мабуть не логічним. За думкою автора, інформаційна безпека, крім захисту інформації (інформаційного ресурсу суб’єкта підприємництва), має бути спрямована на мінімізацію інформаційного ризику, ще має вирішальне значення для управління господарюючими суб’єктами та забезпечення їх розвитку. Враховуючи, ще інформаційні технології можуть являти собою вид інтелектуальної зброї і негативно впливати на підприємницьку діяльність окремих суб’єктів. Інформаційна безпека має включати в себе функції з протидії інформаційно-психологічному впливу, використанню технологій маніпулювання індивідуальною та колективною свідомістю. При тому підході *інформаційну безпеку підприємницької діяльності можна розуміти, як стан інформаційної роботи суб’єктів підприємництва за якого забезпечується ефективне інформаційне супроводження їх діяльності, надійний захист інформаційного ресурсу та результативна протидія негативному інформаційно-психологічному впливу на них.*

Тобто, структуру інформаційної безпеки суб’єкта підприємництва складають три складові, наведені на рис. 1.1.

Враховуючи динамічний характер сучасного інформаційного простору, такий підхід до розуміння суті та змісту інформаційної безпеки забезпечує суб’єктам підприємництва необхідний рівень живучості у їх конкурентній боротьбі, більш оптимальну поведінку у взаємовідносинах поміж собою, іншими організаціями та інституціями. Інформаційна безпека у такому розумінні виступає формою існування суб’єктів підприємництва у інформаційному середовищі.

Інформаційна безпека суб’єкта підприємництва

Протидія негативному інформаційному впливу

Захист інформаційного ресурсу

Інформаційне забезпечення діяльності

Рис. 1.1. Структура інформаційної безпеки суб’єкта підприємництва

*Метою інформаційної безпеки* у такому випадку є виключення можливості втрати суб’єктами підприємництва свого інформаційного ресурсу чи його руйнування, заподіяння шкоди їх іміджу, а також формування умов для ефективної діяльності і отримання прибутку. Критерієм же ефективності інформаційної безпеки є стабільність оцінки діяльності суб’єктів підприємництва на ринку та позитивні перспективи їх розвитку.

Очевидно, що досягнення визначеної мети інформаційної безпеки має забезпечуватись *виконанням певних завдань*, серед яких:

* організація відповідного режиму функціонування інформації в діяльності суб’єктів підприємництва;
* формування, необхідного для забезпечення ефективної діяльності суб’єктів підприємництва, інформаційного ресурсу;
* своєчасне виявлення загроз інформаційному ресурсу та іміджу суб’єктів підприємництва, їх інформаційним відносинам;
* оперативне реагування суб’єктів підприємництва на зміни та порушення умов інформаційних відносин, спроби посягань на їх інформаційні ресурси та імідж;
* забезпечення інформаційного впливу в необхідних суб’єктам підприємництва сегментах ринку;
* підготовка персоналу суб’єктів підприємництва з питань їх інформаційної безпеки;
* оптимізація заходів та витрат пов’язаних з забезпеченням інформаційної безпеки підприємницької діяльності.

Зазначені завдання мають бути інтегровані у повсякденну діяльність суб’єктів підприємництва шляхом планової роботи як спеціальних підрозділів інформаційної безпеки, так і всіх інших, що входять до складу організаційної структури суб’єктів. Останні мають забезпечувати свою інформаційну безпеку всією сукупністю своїх економічних, інтелектуальних, технічних, кадрових можливостей.

Організація інформаційної безпеки суб’єктів підприємництва здійснюється на основі принципу централізованого управління стратегічним розвитком суб’єктів і їх безпеки, як правило, у сукупності заходів, що виконуються ними у сфері забезпечення їх безпеки.

Основними принципами тут виступають:

* *законність* – заходи, що виконуються в межах організації та здійснення інформаційної безпеки мають вкладатись в межі чинного законодавства, не порушувати права та свободи громадян, законні інтереси інших суб’єктів та держави;
* *самостійність та відповідальність* – заходи інформаційної безпеки обираються суб’єктами підприємництва самостійно, в межах своїх можливостей і повинні бути адекватними загрозам їх інформаційній безпеці; за результати вжитих заходів відповідальність покладається на суб’єктів підприємництва та уповноважених ними на проведення таких заходів осіб;
* *компетентність –* виконання заходів інформаційної безпеки має здійснюватись грамотно, на високому професійному рівні, підготовленими для цього фахівцями;
* *економічна доцільність –* витрати на організацію та виконання заходів інформаційної безпеки повинні бути адекватними її ефективності, не завдавати шкоди економічному стану суб’єктів підприємництва;
* *цілеспрямованість –* заходи інформаційної безпеки мають здійснюватись у строгій відповідності основним завданням і напрямком діяльності суб’єктів підприємництва;
* *конфіденційність –* переважна сукупність заходів інформаційної безпеки проводиться на конфіденційній основі, інформування про їх проведення та результати, здійснюється лише обмеженому колу осіб.

Надійність та ефективність інформаційної безпеки суб’єктів підприємництва визначається через її відповідність встановленим вимогам, якими можуть бути:

* *безперервність забезпечення інформаційної безпеки –* заходи інформаційної безпеки проводяться з початком її організації і продовжуються протягом всього часу існування суб’єкта підприємництва, посилюючись та послаблюючись в окремих ситуаціях, але без їх припинення;
* *плановість інформаційної безпеки –* встановлення відповідного порядку застосування заходів інформаційної безпеки, який б забезпечував запобіжний характер їх впливу на виникнення небезпек і загроз;
* *конкретність інформаційної безпеки –* заходами безпеки мають бути охоплені конкретні об’єкти та дії суб’єктів підприємництва; заходи безпеки повинні бути пов’язані з конкретними операціями, угодами, відносинами, які здійснюються на даний час суб’єктами підприємництва;
* *активність інформаційної безпеки –* в арсеналі заходів інформаційної безпеки повинні бути як такі, що забезпечують захист інформаційного ресурсу та іміджу суб’єктів підприємництва, так і ті, які спрямовуються на протидію заходом негативного впливу та розкриття їх джерел;
* *комплексність інформаційної безпеки –* передбачає необхідність застосування у забезпеченні безпеки різних форм, методів, засобів, заходів щодо різних видів інформації та інформаційних відносин.

Реалізація принципів і вимог до інформаційної безпеки неможлива без конкретизації самого об’єкта безпеки. Враховуючи багатофункціональність інформації можна бачити її присутність у будь-якому матеріальному чи нематеріальному об’єкті або у будь-якому виду діяльності. Тобто, будь-який об’єкт чи діяльність можна подати інформаційно, зробити уявлення про нього на основі його інформаційних характеристик. Таким чином, беручи за об’єкт інформаційної безпеки інформацію, маємо обов’язково пов’язати її з певним об’єктом (людиною, підприємством, установою, організацією, предметом) або ж з відповідним видом діяльності. Тоді об’єктом буде виступати уже не інформація як така, а інформація про щось (об’єкт чи діяльність). Разом з тим, інформація про щось може бути об’єктом інформаційної безпеки лише тоді коли вона буде мати певну цінність (для підприємництва – комерційну цінність) і щодо неї буде проявлена зацікавленість з боку інших осіб. Враховуючи наведене, інформацію як об’єкт інформаційної безпеки можна подати наступним чином – Рис. 1.2.

Інформація

Документи

Ділові взаємовідносини

Нові товари та послуги

Технології виробництва

Знання

Електронні носії інформації

Рис. 1.2. Інформація як об’єкт інформаційної безпеки

У практиці забезпечення інформаційної безпеки суттєве значення має визначення її видів. Особливо це необхідно з т. з. організації інформаційної безпеки в діяльності суб’єктів підприємництва.

Аналізуючи практику інформаційних відносин суб’єктів підприємницької діяльності та беручи до уваги роль інформації в такій діяльності, можна говорити, що інформаційна безпека підприємництва включає наступні її види: комп’ютерну безпеку, інформаційно-психологічну безпеку, комунікаційну безпеку та документаційну безпеку.

**Комп’ютерна безпека** передбачає: захист засобів комп’ютеризації, комп’ютерних технологій і інформації, що знаходиться на електронних носіях; отримання необхідної суб’єктам підприємництва інформації із глобального інформаційного простору (мережі Інтернет) для формування їх інформаційного ресурсу; протидія інформаційним загрозам в середовищі електронної інформації(комп’ютерні віруси, шкідливі програми, комп’ютерний тероризм і т. п.)

**Інформаційно-психологічна** безпека зосереджує свої зусилля у сфері знанієвої інформації та її носіїв (працівників, клієнтів, споживачів продукції суб’єктів підприємництва). Основними напрямками забезпечення інформаційної безпеки є захист знаннєвої інформації (організація захисту інтелектуальної власності, режиму використання інформації працівниками та іншими особами у процесі інформаційних відносин); збереження інформаційного здоров’я працівників суб’єктів підприємництва в умовах інформатизації виробництва; розробка технологій отримання знаннєвої інформації (наукові дослідження, конференції, семінари, курси, сімпозіуми і т. п.) для формування інформаційного ресурсу суб’єктів підприємництва; протидія технологіям маніпулювання інформацією, індивідуальною та колективною свідомістю.

**Комунікаційна** безпека включає захист інформації в процесі взаємообміну (електронна пошта, мобільний зв'язок) та ділового спілкування (зустрічі, перемовини); проведення заходів пропаганди, контр-пропаганди та агітації в інформаційному середовищі суб’єктів підприємництва; протидія поширенню негативної інформації засобами масової комунікації.

**Документаційна** безпека спрямована перш за все на захист документованої інформації та її носіїв, насамперед через запровадження надійної системи загального і спеціального діловодства, розробки нормативних документів з питань інформаційної безпеки; запровадження технологій отримання необхідних даних з різного роду документів (правових актів, звітів, звичайних публікацій, виступів, описів і т. п.) для формування інформаційного ресурсу суб’єктів підприємництва; документальне супроводження протидії інформаційним загрозам та інформаційно-психологічному впливу щодо суб’єктів підприємництва, їх діяльності та персоналу(документування фактів порушення інформаційного режиму, поширення неправдивої інформації чи маніпулювання нею, документальне спростування негативної інформації, документи щодо вимог відшкодування моральної шкоди і т. і.)

Фундаментом успіху інформаційної безпеки є грамотна її організація в діяльності суб’єктів підприємництва. На жаль необхідно констатувати, що саме організація на сьогодні є одним із найбільш слабких місць у забезпеченні інформаційної безпеки підприємницької діяльності. Немає таємниці в тому, що саме грамотно організована інформаційна безпека є запорукою успіху суб’єктів підприємництва у їх інформаційних відносинах і діяльності взагалі. Організація інформаційної безпеки є елементом управління безпекою кожного із суб’єктів підприємництва. Тому цим питанням має опікуватись насамперед їх керівництво. Так, з питань організації інформаційної безпеки керівники установ суб’єктів підприємництва мають визначити мету безпеки, її основні завдання та напрямки зосередження основних зусиль; створити сприятливі умови для діяльності сил інформаційної безпеки відповідно до функцій покладених на неї; забезпечувати контроль ефективності функціонування системи інформаційної безпеки суб’єктів підприємництва. Безпосереднім організатором інформаційної безпеки є керівник підрозділу безпеки суб’єкта підприємництва, а там де він відсутній – сам керівник суб’єкта.

Аналіз практики забезпечення інформаційної безпеки в підприємницькій діяльності показує, що питанням її організації не придається необхідного значення, в більшості випадків керівники підрозділів безпеки ними володіють майже на примітивному рівні. Процес організації практично відсутній у керівництві інформаційною безпекою суб’єктів підприємництва. Здебільшого організація безпеки зводиться до реакції на негаразди, які виникають у інформаційних відносинах суб’єктів підприємництва. Потенціал, закладений у грамотній організації інформаційної безпеки, не сприймається як перевага в інформаційному середовищі, конкурентній боротьбі, ринкових відносинах взагалі.

За результатами узагальнення діяльності суб’єктів підприємництва по забезпеченню їх інформаційної безпеки автором запропоновано відповідну структуру процесу її організації на підприємствах, у банках та інших організаціях( Рис. 1.3).

Організація інформаційної безпеки

1. Вивчення інформаційних потреб та загроз інформації суб’єкта підприємництва

2. Визначення мети і завдань інформаційної безпеки суб’єкта підприємництва

3. Визначення складу сил та засобів інформаційної безпеки, розробка їх організаційно – штатної структури

4. Розробка заходів інформаційної безпеки та розрахунок обсягів і порядку їх фінансування

5. Комплектування підрозділів інформаційної безпеки кадрами та необхідними засобами

6. Розробка нормативної бази з питань інформаційної безпеки суб’єкта підприємництва

9. Організація фінансового, матеріального, кадрового, інформаційного, наукового забезпечення діяльності сил інформаційної безпеки

8. Організація взаємодії підрозділів інформаційної безпеки з іншими підрозділами суб’єкта підприємництва

7. Планування заходів інформаційної безпеки в діяльності суб’єкта підприємництва

10. Контроль ефективності виконання заходів інформаційної безпеки в діяльності суб’єкта підприємництва

Рис. 1.3. Структура процесу організації інформаційної безпеки суб’єкта підприємництва

Процес організації інформаційної безпеки суб’єкта підприємництва виконується на підставі глибокого вивчення умов та змісту діяльності суб’єкта, характеру його взаємовідносин на ринку та поведінки в інформаційному середовищі. Крім того, процесу організації мають передувати вивчення можливостей суб’єкта підприємництва щодо забезпечення відповідного рівня інформаційної безпеки та правових умов в яких здійснює свою діяльність суб’єкт. Процедура та зміст організації інформаційної безпеки обов’язково має бути узгоджена з точкою зору керівника установи суб’єкта підприємництва. Точка зору керівника має бути сформована як його рішення з даного питання.

Важливим в організації інформаційної безпеки суб’єктів підприємництва залишається створення відповідної системи. Остання має розумітись як певна сукупність сил, засобів, заходів і технологій, спрямованих на забезпечення високої стійкості суб’єкта підприємництва до інформаційних загроз та ефективне інформаційне супроводження його діяльності.

Основними принципами побудови системи інформаційної безпеки мають виступати:

* *стійкість* – система має ефективно протистояти будь-яким діям, спрямованим на її руйнування чи дестабілізацію функціонування;
* *адаптація* – система має оперативно реагувати на будь-які зміни в інформаційному середовищі та інформаційних відносинах суб’єкта підприємництва;
* *трансформація* – система має працювати з різними видами інформації, в різних інформаційних середовищах, в будь-яких комунікаційних мережах без втрати ефективності забезпечення інформаційної безпеки суб’єкта підприємництва;
* *відновлення* – система має бути здатною в оптимально короткі терміни відновлювати свою живучість та забезпечувати виконання необхідного обсягу заходів інформаційної безпеки суб’єкта підприємництва обмеженим складом сил і засобів;
* *автономність* – система має бути максимально незалежною від зовнішніх джерел та суб’єктів, забезпечувати своє функціонування власними силами та засобами.

Таким чином, враховуючи структуру та зміст завдань інформаційної безпеки, обсяг заходів, які покладаються на неї, можна стверджувати, що вона займає одне із провідних місць у забезпеченні безпеки діяльності суб’єктів підприємництва. В той же час, забезпечення інформаційної безпеки це досить складний і трудомісткий процес, який вимагає значних фінансових, матеріальних, інтелектуальних зусиль. Останні ж мають спиратись на грамотні, науково обґрунтовані та підтверджені підприємницькою практикою погляди професіоналів, здатних реалізувати визначену певним суб’єктом підприємництва концепцію інформаційної безпеки.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Процес організації інформаційної безпеки суб’єкта підприємництва виконується на підставі глибокого вивчення умов та змісту діяльності суб’єкта, характеру його взаємовідносин на ринку та поведінки в інформаційному середовищі.

**ВИСНОВКИ З ТЕМИ**

Таким чином, враховуючи структуру та зміст завдань інформаційної безпеки, обсяг заходів, які покладаються на неї, можна стверджувати, що вона займає одне із провідних місць у забезпеченні безпеки діяльності суб’єктів підприємництва. В той же час, забезпечення інформаційної безпеки це досить складний і трудомісткий процес, який вимагає значних фінансових, матеріальних, інтелектуальних зусиль. Останні ж мають спиратись на грамотні, науково обґрунтовані та підтверджені підприємницькою практикою погляди професіоналів, здатних реалізувати визначену певним суб’єктом підприємництва концепцію інформаційної безпеки.

**ТЕМА 2. ЗАГРОЗИ БЕЗПЕЦІ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ**

**ПЛАН ЛЕКЦІЇ:**

1. Базові терміни та визначення.

2. Класифікація загроз безпеці.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

Конституція України від 28.06.1996 № 254к/95-ВР (Редакція від 21.02.2019).

Закони:

* Закон України «Про інформацію» від 02.10.1992 № 2657-XII
* Закон України «Про захист інформації в інформаційно-телекомунікаційних
* системах» від 05.07.1994 № 80/94-ВР
* Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
* Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Нормативні документи:

* НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
* Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
* НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
* НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
* НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

**Навчальні посібники, інші дидактичні та методичні матеріали:**

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем.–М.: ГТУим. Н.Э. Баумана, 2016.–252с.

1. Інформаційне забезпечення юридичної діяльності: підручник / кол. авт.; ред. В.Б. Вишня. - Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. - 245 с.

3. Інформатика і комп’ютерна техніка : навч. посіб. / Л.М.Дибкова. – 3-тє вид., доп. –.К.: Академвидав, 2011. – 464 с.

4. Інформатика в юридичній діяльності / Кудінов В.А., Хахановський В.Г., Пакриш О.Є. та ін. за заг. редакцією В.А. Кудінова. – К.: Нац. акад. внутр. справ, 2016. – 256 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2004.

**МЕТА ЛЕКЦІЇ:**

Познайомити студентів з загрозами безпеки підприємницької діяльності. Зрозуміти базові терміни та визначення загроз безпеці підприємницької діяльності.

**ВСТУП**

Підприємництво представляє собою ініціативну самостійну діяльність громадян або їх об’єднань, що здійснюється на свій страх і ризик, під свою майнову відповідальність і спрямовується на отримання прибутку. Часто підприємн6ицьку діяльність називають бізнесом. Підприємництво є основою інноваційного, продуктивного характеру економіки. Створені ним дрібні та середні підприємства забезпечують освоєння нових перспективних виробництв, сприяють відмиранню застарілих технологій та розвитку конкуренції, а також збільшенню відкритості національної економіки, ввезенню та вивезенню капіталу. Саме підприємництво створює механізм координації, розробки стратегії розвитку через ринок і конкуренцію та зв’язки між господарюючими суб’єктами.

1. **Базові терміни та визначення**

 *Інформаційний простір* — середовище, де здійснюється формування, збір,

зберігання та розповсюдження інформації.

 *Інформаційний ресурс* — це складова інформаційного простору, що

поєднує в собі дані, їх місцезнаходження, взаємозв’язок між інформаційними

елементами, відомості (про процеси надходження, зберігання, обробки тощо).

 *Інформаційна інфраструктура* — це складова інформаційного

простору, яка являє собою сукупність даних (структурованих чи неструктурованих); засобів збору, накопичення, обробки, збереження та

розповсюдження інформації; системи виробництва інформаційних продуктів; інформаційних ресурсів зовнішнього інформаційного простору; інструктивних матеріалів та документації; людини як активного фактору вплину на інформаційний простір.

 *Інформаційна безпека* — стан захищеності інформаційного

простору, який забезпечує формування та розвиток цього простору в

інтересах особистості, суспільства та держави.

Об'єкт інформаційної безпеки. Соціальними об'єктами інформаційної

безпеки є: особа — її права та свободи в інформаційній сфері; суспільство — його духовні цінності, засади солідарної діяльності; держава — її конституційний лад, суверенітет, ефективне функціонування.

Технічними об'єктами інформаційної безпеки є інформаційні ресурси,

інформаційна інфраструктура, інформаційні технології.

 Загрози інформаційній безпеці — фактор або їх сукупність, що створюють

небезпеку функціонуванню та розвитку інформаційного простору, інтересам особистості, суспільства, держави.

 *Захист інформації* — сукупність засобів, методів, організаційних

заходів щодо попередження можливих випадкових або навмисних впливів

природного чи штучного характеру, наслідком яких може бути нанесення

збитків чи шкоди власникам інформації або її користувачам, інформаційному

простору. Суттю захисту інформації є її доступність при збереженні цілісності

інформації та гарантованій конфіденційності.

*До основних задач забезпечення інформаційної безпеки належать:*

 • виявлення, оцінка та прогнозування джерел загроз інформаційній

безпеці;

 • розробка державної політики забезпечення інформаційної безпеки та комплексу заходів і механізмів її реалізації;

 • створення нормативно-правових засад забезпечення інформаційної безпеки, координація діяльності органів державної влади та управління, установ та підприємств по реалізації політики інформаційної безпеки;

 • розвиток системи забезпечення інформаційної безпеки,

вдосконалення її організації, форм, методів і засобів запобігання загрозам

інформаційній безпеці та ліквідації наслідків її порушення;

 • забезпечення участі в процесах створення і використання глобальних інформаційних мереж та систем.

 **ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Інформаційна безпека відіграє суттєву роль в забезпеченні життєво

важливих інтересів будь-якої країни.

Метою забезпечення інформаційної безпеки в Україні є створення розгалуженого та захищеного інформаційного простору, захист національних інтересів України в умовах формування світових інформаційних мереж, захист економічного потенціалу держави від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ та держави на отримання, поширення та використання інформації.

1. **Класифікація загроз безпеці.**

До джерел загроз належать:

 • недружня політика іноземних держав в галузі глобального інформаційного моніторингу, поширення інформації та новітніх інформаційних технологій;

• цілеспрямована діяльність іноземних спецслужб, політичних та

економічних структур;

• злочинна діяльність міжнародних угрупувань, формувань та окремих осіб;

• неправомірна чи протиправна діяльність посадових осіб державних

органів, структур, формувань, спрямована проти інтересів України;

• стихійні лиха, катастрофи, збройні конфлікти;

• недосконалість технічних і програмних засобів та недостатня кваліфікація персоналу інформаційних служб і систем;

• недосконалість, неповнота і неузгодженість з відповідними

міжнародними правовими актами чинного законодавства України в

інформаційній сфері;

• недостатній розвиток лексикографічної бази української мови і національного лінгвістичного забезпечення інформаційних систем;

• низькі темпи науково-технічного і культурного розвитку суспільства

внаслідок економічної кризи або неадекватної внутрішньої політики держави

в інформаційній сфері;

• низька правова, організаційна та програмно-технічна забезпеченість

в галузі інформаційної безпеки.

*Засоби впливу* загроз на інформаційну безпеку поділяються на

інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-

правові.

*До інформаційних засобів належать:*

* порушення адреси і своєчасності інформаційного обміну,
* протизаконні збір і використання інформації;
	+ - несанкціонований доступ до інформаційних ресурсів;
		- маніпулювання інформацією (дезінформація, укриття та викривлення інформації);
		- незаконне копіювання інформації в інформаційних системах;
* використання засобів масової інформації з позицій, які суперечать
* інтересам громадян, організацій чи держави;
	+ - викрадення інформації з бібліотек, архівів, банків і баз даних;
		- порушення технології обробки інформації.

*До програмно-математичних засобів належать:*

* запуск програм-вірусів; установка програмних і апаратних закладних пристроїв;
* знищення і модифікація даних в інформаційних системах.

*Фізичні засоби включають:*

* знищення або руйнування засобів обробки інформації і зв’язку;
* знищення, руйнування чи викрадення оригінальних носіїв
* інформації;
* викрадення програмних чи апаратних ключів і засобів криптографічного захисту інформації;
* вплив на персонал; поставка ―інфікованих компонентів інформаційних систем.

 *До радіоелектронних засобів належать:*

* перехоплення інформації в технічних каналах її витоку;
* будова електронних пристроїв перехоплення інформації в технічних

засобах і приміщеннях;

* перехоплення, дешифрування та подання хибної інформації в мережах передачі даних і мережах зв’язку;
* вплив на парольно-ключові системи;
* радіоелектронне придушення мереж зв’язку і систем керування.

 *До організаційно-правових засобів*

* слід віднести купівлю недосконалих або застарілих інформаційних технологій та засобів інформатизації;
* невиконання вимог законодавства та затримку прийняття необхідних нормативно-правових положень в інформаційній сфері;
* неправомірне обмеження доступу, до документів, в яких знаходиться важлива для громадян та організацій інформація.

 Реалізація інформаційних загроз на рівні особи призводить до порушення або обмеження доступу громадян до інформації загального

користування. Це створює загрозу інформаційній безпеці особистості як з боку органів влади, так і з боку сторонніх осіб або угрупувань, порушує баланс стосунків між особистістю, суспільством і державою.

 Наслідком впливу інформаційних загроз на соціальну спільноту є ускладнення соціальних процесів, що виявляється у загостренні суперечностей між різними соціальними прошарками, загостренні політичної боротьби, розпалюванні релігійних та етнічних суперечностей, зниженні загальної культури населення, розвитку бездуховності, зростанні злочинності, розповсюдженні антигуманних ідей.

 Наслідки інформаційних злочинів в економічній сфері можуть призвести до економічних втрат за рахунок знецінення і втрати товарної частини інформаційного ресурсу — промислових і інформаційних технологій.

*Методи запобігання та ліквідації загроз інформаційній безпеці*

 Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмно-технічні і організаційно-економічні методи.

 Правові методи - передбачають розробку комплексу нормативно-

правових актів і положень, регламентуючих інформаційні відносини

в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки.

 *Програмно-технічні методи — це сукупність засобів:*

 • запобігання витоку інформації,

 • виключення можливості несанкціонованого доступу до інформації,

 • запобігання впливам, які призводять до знищення, руйнування,

спотворення інформації, або збоям чи відмовам у функціонуванні засобів

інформатизації,

 • виявлення закладних пристроїв,

 • виключення перехоплення інформації технічними засобами,

 • використання криптографічних засобів захисту інформації при передачі

по каналах зв’язку.

 Організаційно-економічні методи перед6ачають формування і

забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих систем згідно вимогам інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту інформації, контроль за діями персоналу в захищених інформаційних системах.

*Організаційні основи захисту інформації*.

 В загальному принципи захисту інформації можна умовно розділити на дві основні групи:

* правові принципи;
* організаційні принципи;

Правові принципи захисту інформації

Правове регулювання захисту інформації спирається на принципи інформаційного права. Дані принципи, що базуються на положеннях

основних конституційних норм, закріплюють інформаційні права і свободи, а так само гарантують їх здійснення. Крім того, основні правові засади захисту

інформації ґрунтуються на особливостях і юридичних властивостях

інформації як повноцінного об'єкту правовідносин.

Узагальнено до правових принципів захисту інформації відносяться:

* легітимність (законність);
* пріоритет міжнародного права над внутрішньодержавним;
* економічна доцільність.

*Організаційні принципи захисту даних*

Роль організаційного захисту інформації в системі заходів безпеки

визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-

методичних документів.

Організаційні методи захисту передбачають проведення організаційно-

технічних та організаційно-правових заходів, а так само включають в себе наступні принципи захисту інформації:

* науковий підхід до організації захисту інформації;
* планування захисту ;
* керування системою захисту;
* безперервність процесу захисту інформації;
* мінімальна достатність організації захисту;
* системний підхід до організації та проектування систем та методів
* захисту інформації;
* комплексний підхід до організації захисту інформації;
* відповідність рівня захисту цінності інформації;
* гнучкість захисту;
* багатозональність захисту, що передбачає розміщення джерел

інформації в зонах з контрольованим рівнем її безпеки;

* багаторубіжність захисту інформації;
* обмеження числа осіб, які допускаються до захищеної інформації;
* особиста відповідальність персоналу за збереження довіреної інформації.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Після завершення атестації комплексу оформляється технічний паспорт на комплекс ТЗІ і готується наказ (розпорядження) керівника установи щодо готовності ОІД до озвучення та (або) оброблення ІзОД технічними засобами (крім оброблення ІзОД в АС: дозвіл на обробку ІзОД в АС готується за результатами проведення державної експертизи КСЗІ в АС).

**ВИСНОВКИ З ТЕМИ**

Загрози можна розглядати також з точки зору характеру відповідальності суб’єкта, дії якого можуть кваліфікуватись як зазіхання на економічну безпеку підприємницької діяльності. Відповідальність, що наступає у цих випадках носить або цивільно-правовий або кримінально-правовий характер і тягне за собою відповідні заходи до осіб, що їх скоїли.

**ТЕМА 3. ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА**

**ПЛАН ЛЕКЦІЇ:**

1. Поняття права інтелектуальної власності. Суб'єкти і об'єкти права інтелектуальної власності. Підстави виникнення права інтелектуальної власності. Захист права інтелектуальної власності

2. Методи захисту інформації.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

Конституція України від 28.06.1996 № 254к/95-ВР (Редакція від 21.02.2019).

Закони:

* Закон України «Про інформацію» від 02.10.1992 № 2657-XII
* Закон України «Про захист інформації в інформаційно-телекомунікаційних
* системах» від 05.07.1994 № 80/94-ВР
* Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
* Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Нормативні документи:

* НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
* Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
* НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
* НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
* НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

**Навчальні посібники, інші дидактичні та методичні матеріали:**

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем.–М.: ГТУим. Н.Э. Баумана, 2016.–252с.

1. Інформаційне забезпечення юридичної діяльності: підручник / кол. авт.; ред. В.Б. Вишня. - Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. - 245 с.

3. Інформатика і комп’ютерна техніка : навч. посіб. / Л.М.Дибкова. – 3-тє вид., доп. –.К.: Академвидав, 2011. – 464 с.

4. Інформатика в юридичній діяльності / Кудінов В.А., Хахановський В.Г., Пакриш О.Є. та ін. за заг. редакцією В.А. Кудінова. – К.: Нац. акад. внутр. справ, 2016. – 256 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2004.

**МЕТА ЛЕКЦІЇ:**

Зрозуміти такі поняття як інтелектуальна власність, захист права інтелектуальної власності, службова та комерційна таємниця.

**ВСТУП**

Інтелектуальна власність - збірне поняття, що означає сукупність виняткових прав на результати творчої діяльності і засоби індивідуалізації. Охоплює права, що відносяться до літературних, художніх і наукових творів, виконавської діяльності артистів, звукозапису, радіо - і телепередач, винаходів, промислових зразків, товарних знаків, фірмових найменувань і т.п.

1. **Поняття права інтелектуальної власності. Суб'єкти і об'єкти права інтелектуальної власності. Підстави виникнення права інтелектуальної власності. Захист права інтелектуальної власності.**

Праву інтелектуальної власності присвячена книга 4 Цивільного кодексу України. Крім ЦК право інтелектуальної власності регулюється спеціальними нормативно-правовими актами, такими як: ЗУ "Про авторське право і суміжні права" від 23 грудня 1993 р., ЗУ "Про охорону прав на винаходи і корисні моделі" від 1 червня 2000 р., ЗУ "Про охорону прав на промислові зразки" від 15 грудня 1993 р. та ін.

Право інтелектуальної власності - це право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності, визначений цим Кодексом та іншим законом (ст. 418 ЦК).

Право інтелектуальної власності становлять особисті немайнові права інтелектуальної власності та (або) майнові права інтелектуальної власності, зміст яких щодо певних об'єктів права інтелектуальної власності визначається цим Кодексом та іншим законом.

Право інтелектуальної власності є непорушним. Ніхто не може бути позбавлений права інтелектуальної власності чи обмежений у його здійсненні, крім випадків, передбачених законом.

Інтелектуальна власність - збірне поняття, що означає сукупність виняткових прав на результати творчої діяльності і засоби індивідуалізації. Охоплює права, що відносяться до літературних, художніх і наукових творів, виконавської діяльності артистів, звукозапису, радіо - і телепередач, винаходів, промислових зразків, товарних знаків, фірмових найменувань і т.п.

Інтелектуальна власність поділяється на "промислову власність" і "авторське право".

Промислова власність - юридичне поняття, що охоплює права на такі результати інтелектуальної діяльності як винахід, корисні моделі, промислові зразки, товарні знаки та інші об'єкти, передбачені Паризькою конвенцією по охороні промислової власності.

Авторське право - надає авторам та іншим творцям інтелектуальних творів (література, музика, мистецтво) певні права, згідно з якими вони мають можливість дозволяти або забороняти протягом певного обмеженого періоду часу ті або інші види використання їх творів. Авторське право включає охорону "суміжних прав".

До об'єктів права інтелектуальної власності, зокрема, належать (ст.420ЦК):

* - літературні та художні твори;
* - комп'ютерні програми;
* - компіляції даних (бази даних);
* - виконання;
* - фонограми, відеограми, передачі (програми) організацій мовлення;
* - наукові відкриття;
* - винаходи, корисні моделі, промислові зразки;
* - компонування (топографії) інтегральних мікросхем;
* - раціоналізаторські пропозиції;
* - сорти рослин, породи тварин;
* - комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення;
* - комерційні таємниці.

Суб'єктами права інтелектуальної власності є: творець (творці) об'єкта права інтелектуальної власності (автор, виконавець, винахідник тощо) та інші особи, яким належать особисті немайнові та (або) майнові права інтелектуальної власності відповідно до цього Кодексу, іншого закону чи договору.

Суб'єктом права інтелектуальної власності, перш за все, є творець такого результату. Творцем може бути лише фізична особа, юридичні ж особи можуть стати суб'єктами права інтелектуальної власності на підставі закону.

Всі суб'єкти права інтелектуальної власності можна поділити на первинних і похідних. До перших відносяться лише творці результату інтелектуальної діяльності. Похідними є всі правонаступники, до яких право інтелектуальної власності перейшло на підставі договору або в силу закону. Первинний суб'єкт права може передати свої майнові права на об'єкт інтелектуальної власності будь-якій іншій особі.

Окремою категорією суб'єктів є роботодавці, у яких виникає право інтелектуальної власності на об'єкти, які створені при виконанні службових обов'язків. Так, в разі коли об'єкт інтелектуальної власності створено при виконанні трудового договору, то право на нього належить як працівникові, що створив об'єкт, так і роботодавцю, в той же час сторони можуть визначити інший порядок.

Якщо об'єкт інтелектуальної власності створено в результаті участі кількох осіб, то всі вони є суб'єктами права інтелектуальної власності, а саме співавторами.

Статтею 422 ЦК не встановлено підстав виникнення (набуття) права інтелектуальної власності, а лише визначено, що "Право інтелектуальної власності виникає (набувається) з підстав, встановлених цим Кодексом, іншим законом чи договором". Право інтелектуальної власності на результат творчої діяльності виникає внаслідок його створення, якщо такий об'єкт відповідає вимогам закону, а саме він має бути новим, втіленим в матеріальний об'єкт, придатним для використання, та відповідати іншим вимогам встановленим законодавством.

Законом можуть бути передбачені й інші підстави виникнення права інтелектуальної власності на об'єкт, а саме з моменту реєстрації майнових прав або внаслідок використання.

Внаслідок створення виникають авторські і суміжні права. Право інтелектуальної власності на об'єкти суміжних прав виникають, щодо виконань - з моменту їх першого здійснення, щодо фонограм і відеограм - з моменту їх вироблення, щодо передач - з моменту їх першого здійснення.

Що стосується об'єктів права промислової власності, то момент виникнення права інтелектуальної власності встановлено законодавством щодо кожного окремого об'єкта, що знайшло своє відображення в спеціальних статтях Цивільного кодексу України, що регулюють відносини, які виникають у зв'язку з тим чи іншим об'єктом.

Крім того, майнові права на об'єкти інтелектуальної власності можуть переходити до третіх осіб на підставі цивільно-правових договорів. Такі права можуть бути передані повністю або частково. Також окремою підставою виникнення права інтелектуальної власності може бути перехід такого права у спадщину.

У випадку порушення права інтелектуальної власності кожна особа, згідно із ст. 16 Цивільного кодексу України, може звернутися до суду за захистом свого права. Стаття 432 ЇДКУ передбачає особливі способи захисту порушеного права інтелектуальної власності. Результати інтелектуальної діяльності стають об'єктами правової охорони, якщо вони відповідають вимогам закону.

Кожна особа має право звернутися до суду за захистом свого права інтелектуальної власності відповідно до статті 16 цього Кодексу.

Суд у випадках та в порядку, встановлених законом, може постановити рішення, зокрема, про:

* - застосування негайних заходів щодо запобігання порушенню права інтелектуальної власності та збереження відповідних доказів;
* - зупинення пропуску через митний кордон України товарів, імпорт чи експорт яких здійснюється з порушенням права інтелектуальної власності;
* - вилучення з цивільного обороту товарів, виготовлених або введених у цивільний оборот з порушенням права інтелектуальної власності, та знищення таких товарів;
* - вилучення з цивільного обороту матеріалів та знарядь, які використовувалися переважно для виготовлення товарів з порушенням права інтелектуальної власності, або вилучення та знищення таких матеріалів та знарядь;
* - застосування разового грошового стягнення замість відшкодування збитків за неправомірне використання об'єкта права інтелектуальної власності. Розмір стягнення визначається відповідно до закону з урахуванням вини особи та інших обставин, що мають істотне значення; - опублікування в засобах масової інформації відомостей про порушення права інтелектуальної власності та зміст судового рішення щодо такого ***порушення.***

Сектор ділової інформації, представлений такими видами і джерелами як біржова, фінансова, економічна, статистична та комерційна інформація. Поряд із факторами, які забезпечують комерційну цінність інформації (повнота, точність, оперативність), особливого значення набуває доступність її для споживача. Цінністю володіє тільки та інформація, яку можна використовувати. З цього моменту все залежить від того в яких або в чиїх цілях буде використана інформація, а тому яку інформацію можна передавати відкрито, а яку потрібно оберігати, зробити з неї таємницю.

**Службову таємницю** організації становлять відомості про фінанси та бюджетну політику, відомості про організацію внутрішньовиробничої та управлінської діяльності із забезпечення захисту цих відомостей відповідно до норм діючого законодавства. Такими відомостями є:

− відомості щодо пропозицій організації до проектів документів на державному рівні;
− внутрішні квартальні, піврічні та річні звіти про результати діяльності організації;
− відомості про технічні заходи підприємств із забезпечення інформаційної безпеки;

− матеріали, у яких визначається стратегія на майбутній рік і на більш далеку перспективу;
− внутрішні довідки про результати діяльності організації;

− доповідні записки на ім’я керівництва організації з основних напрямів діяльності;
− інструкції, розроблені в організації;

− доповідні записки на ім’я керівництва організації за матеріалами ревізій структурних підрозділів, що містять висновки та пропозиції, пов’язані з діями посадових осіб;

− прогнози різноманітного характеру;

− штатний розклад організації;

− телефонний довідник організації;

− відомості про партнерів;

− документи з охорони і захисту конфіденційних відомостей;

− відомості, які розкривають систему захисту конфіденційної інформації, в тому числі, при використанні електронних технологій;

− листування організації з правоохоронними органами;

− рахунок прибутків і видатків організації;

− матеріали ревізій, що проводились в організації та у підвідомчих закладах;

− система розмежування повноважень на інформаційному об’єкті;

− паролі та ідентифікатори клієнтів, працівників, використовувані на автоматизованих системах;

− порядок доступу осіб у приміщення з обмеженим доступом;

− проект комплексного захисту інформаційної системи, алгоритми, програми шифрування і дешифрування інформації.

**Комерційну таємницю** становлять економічні інтереси та інформація про різні сфери виробничо-господарської, управлінської, науково-технічної, фінансової діяльності організації, охорона яких обумовлена інтересами конкуренції та можливою загрозою економічній безпеці підприємства.

До таких відомостей відносяться:

− комерційні угоди, укладені організацією;

− угоди з іншими організаціями;

− відомості про перспективні експериментальні розробки до їх впровадження і реклами;
− фінансові документи організації;

− відомості, які надані виконавцями робіт підприємству як конфіденційні, що стосуються комерційних відносин між сторонами;

− відомості про фінансовий стан виконавців;

− зміст переговорів з клієнтами щодо окремих видів робіт і послуг;

− протоколи зустрічей керівників організації з виконавцями з питань організації робіт;

− файли баз даних, що містять конфіденційні відомості;

− внутрішні нормативні документи організації;

− відомості, що розкривають інформацію про фінансовий стан працівників;
− відомості про порушення партнерами договірних зобов’язань, правил роботи, про штрафи і санкції до них;

− відомості про розподіл прибутків;

− відомості про стратегічні і перспективні напрями роботи організації;

− відомості про наявність вільних кредитних ресурсів та їх розміщення;

− умови видачі кредитів конкретним одержувачам (процент кредитної ставки, терміни, застава тощо);

− вартість послуг для конкретного клієнта;

− інженерно-економічні розрахунки і прогнози техніко-економічного стану і розвитку організації.

**Персональна таємниця** – це інформація, яка містить відомості про фізичну особу, і дозволяє цю фізичну особу ідентифікувати. До відомостей, що становлять персональну таємницю, відносяться:

− особова справа працівника організації;

− відомості про клієнтів і працівників після звільнення;

− заходи із забезпечення збереження, цілісності і достовірності персональних даних;
− результати аудиту використання і захисту персональних даних.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Сектор ділової інформації, представлений такими видами і джерелами як біржова, фінансова, економічна, статистична та комерційна інформація. Поряд із факторами, які забезпечують комерційну цінність інформації (повнота, точність, оперативність), особливого значення набуває доступність її для споживача. Цінністю володіє тільки та інформація, яку можна використовувати. З цього моменту все залежить від того в яких або в чиїх цілях буде використана інформація, а тому яку інформацію можна передавати відкрито, а яку потрібно оберігати, зробити з неї таємницю.

1. **Методи захисту інформації**

Засоби захисту інформації обираються відповідно до змісту таких структурних елементів моделі інформаційної безпеки підприємства:

**Об’єкти злочинних посягань**

* технологічний процес опрацювання, передачі та зберігання інформації;
* інформаційні ресурси.

**Перелік загроз**

− порушення термінів і порядку проходження документів;

− викривлення, фальсифікація, переадресування, несанкціоноване знищення, неправдива авторизація документів та повідомлень, які зберігаються у системі;
− порушення конфіденційності інформації, яка віднесена до комерційної таємниці.

**Можливі суб’єкти, що здійснюють злочинні посягання.**

− співробітник підприємства, який має повноваження доступу до інформаційної системи підприємства;

− співробітник підприємства, який не має повноважень доступу до інформаційної системи підприємства;

− особа, яка не є співробітником підприємства і не має повноважень доступу до інформаційної системи.

**Можливі типи структурних посягань у інформаційній системі підприємства**

− втручання у технологічний процес опрацювання, зберігання і передавання інформації з метою реалізації злочинного посягання;

− використання санкціонованого користувача для втручання у технологічний процес опрацювання, зберігання і передавання інформації з метою реалізації злочинного посягання.

 **Форми здійснення злочинних посягань**

− змова, яка включає співробітника (співробітників) підприємства як учасника;
− використання співробітника (співробітників) підприємства без їхнього відома;
− здійснення економічного, фізичного або морального тиску на співробітника (співробітників) підприємства;

− імітація із злочинною метою дій санкціонованого користувача, який знаходиться на території підприємства;

− імітація із злочинною метою дій санкціонованого користувача, який знаходиться поза територією підприємства.

 **Група ризику санкціонованих користувачів**

− співробітники підприємства, що задіяні у технологічних процесах опрацювання, передавання і зберігання інформації;

− співробітники підприємства, що не задіяні у технологічних процесах опрацювання, передавання і зберігання інформації, але мають можливість організувати втручання у технологічний процес;

− співробітники організацій, з якими підприємство взаємодіє у процесах обміну інформацією, або співробітник організацій, які є для підприємства виконавцями робіт за угодами на тимчасовій або постійній основі.

 **Група ризику несанкціонованих користувачів**

− Співробітники підприємства, які мають можливість здійснювати економічний, фінансовий або моральний вплив на санкціонованих користувачів інформаційної системи з метою реалізації злочинного посягання у інформаційній сфері;

− Колишні співробітники підприємства або співробітники організацій, які взаємодіють з підприємством, які раніш мали доступ до інформаційної системи;

− Злочинні елементи.

 **Мотиви злочинних посягань**

− економічний;

− емоційний (акт особистої помсти, образа та ін..);

− політичний (з метою завдання шкоди національній системі або країні уцілому).

**Можливі місця здійснення злочинних посягань**

Будівлі, приміщення, технічні засоби (обчислювальна техніка, телекомунікаційне обладнання, канали зв’язку, програмні засоби).

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Слід зауважити, що попередньо працівник обов’язково повинен бути ознайомлений з переліком такої інформації. Адже якщо йому не відомо про те, які відомості належать до комерційної таємниці, то, відповідно, він не несе відповідальності за їх розголошення.

**ВИСНОВКИ З ТЕМИ**

Важливо розрізняти правове регулювання вище названих відносин і такі правові інститути, як службова або комерційна таємниця. Різниця полягає в тому, що цінність службової або комерційної таємниці безпосередньо пов'язана з можливістю використання інформації, наприклад, для удосконалення виробничого процесу, а набуття такої інформації здійснюється з метою досягнення завдяки їй певного результату. В інших випадках інформація має значення для того, хто її набуває, сама по собі, поза зв'язком з можливістю реалізації процесу, який охоплюється цією інформацією. Такі випадки перебувають поза межами службової чи комерційної таємниці.

**ТЕМА 4. ОРГАНІЗАЦІЯ БЕЗПЕКИ В РОБОТІ З ПЕРСОНАЛОМ ПІДПРИЄМСТВА**

**ПЛАН ЛЕКЦІЇ:**

1. Планування персоналу
2. Методи залучення персоналу

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

1. Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. –Львів : Видавництво Львівської політехніки, 2015. –256 с.

2. Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації -Харків: ХНУРЕ, 2004 -368 с.

3. Лагун А. Е. Криптографічні системи та протоколи: нав. посібник / А. Е. Лагун. –Львів : Видавництво Львівської політехніки, 2013. –96 с

4. Інформатика в юридичній діяльності / Кудінов В.А., Хахановський В.Г., Пакриш О.Є. та ін. за заг. редакцією В.А. Кудінова. – К.: Нац. акад. внутр. справ, 2016. – 256 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2014.

**МЕТА ЛЕКЦІЇ:**

Ознайомитись з основними правилами підбору персоналу, їх тестування та планування кадрової політики.

**ВСТУП**

Найчастіше кадрове планування розуміється як процес забезпечення організації необхідною кількістю кваліфікованого персоналу, прийнятого на відповідні посади в потрібний час. Очевидно, що ключовими моментами є саме якісна і кількісна відповідність персоналу фронту робіт. Оскільки реалізація цього тезису залежить від багатьох компонентів, то і визначення кадрового планування стає набагато ширшим. В загальному вигляді кадрове планування – це діяльність організації, спрямована на підготовку кадрів, забезпечення пропорційного і динамічного розвитку персоналу, розрахунок професійно-кваліфікованої структури кадрів, визначення загальної і додаткової потреби в них, контроль використання персоналу.

1. **Планування персоналу**

При плануванні роботи з персоналом необхідно спиратись на реально існуючі особливості політичної, соціальної та демографічної ситуацій, які тісно пов’язані з балансом трудових ресурсів:

* обмеженість припливу, або вивільнення працівників;
* чільні тенденції соціального забезпечення і науково-технічного прогресу;
* зростання вимог до регулювання зайнятості населення і організації управління;
* накопичений досвід реалізації основних напрямків удосконалення роботи з кадрами в попередніх періодах.

Мета таких програм – створити умови для забезпечення виробничих підрозділів стабільними кваліфікованими кадрами, для постійного зростання продуктивності праці за рахунок реалізації заходів програми, зниження рівня плинності кадрів і втрат робочого часу, а також покращення структури кадрів відповідно до вимог розвитку сучасного виробництва.

Єдина система планування роботи з персоналом формується на основі сукупності довгострокових (понад 5 років), середньострокових (від 1 року до 5 років) і поточних (до року) планів. Діяльність з планування роботи з персоналом будується на основі стратегічних і тактичних планів організації, і, відповідно, містить декілька етапів: прогнозування, корекцію та складання безпосередньо плану виконання робіт, який містить:

* прогнози розвитку організації в цілому та її окремих підструктур з метою визначення потреби в кадрах;
* проміжні та кінцеві задачі, що стоять перед службами управління персоналом;
* планування підготовки, перепідготовки і підвищення кваліфікації працівників;
* планування розподілу і перерозподілу кадрів;
* планування підвищення ефективності використання кадрів.

Планування виконується певними методами і базується на ряді принципів.

*Прогноз як етап планування персоналу*

Прогнозування є попередньою стадією планування кадрової роботи. Воно служить основою підготовки планових рішень і завдань. Прогнозування зміни структури і динаміки кадрової роботи проводиться на основі аналізу минулого і сьогодення. Воно враховує цілі розвитку підприємства, які необхідно досягти на певному перспективному етапі. Мета прогнозу полягає в тому, щоб розробити основні передумови для:

* розробки вимог до персоналу;
* пошуку кандидатів зі сторони;
* пошуку кандидатів всередині організації.

Різноманіття факторів, які діють на систему організації ззовні, наявність рухливих зв’язків між окремими ланками структури управління і мінливі пріоритети діяльності обумовлюють динаміку розвитку організації. Тому сутність прогнозу структури кадрів, шляхів її вдосконалення визначається передбаченням змін в системах підбору, підготовки, розстановки і виховання кадрів, станом демографічних змін в регіоні, збільшенням вимог до кадрів і кадрової роботи. Прогнозування будується на основі переробки необхідної інформації, враховується аналіз попиту і пропозиції для визначення економії або надлишку кадрових ресурсів.

Основні етапи прогнозування:

* ретроспекція – вивчення стану кадрової роботи і структури кадрів в минулому, аналіз основних закономірностей і вивчення тенденції зайнятості;
* діагноз – визначення характеру і стану кадрової роботи та структури кадрів на підставі всебічного їх дослідження. Виявляються тенденції в розвитку структури кадрів, визначаються шляхи вдосконалення кадрової роботи, цілі прогнозування і коло кадрових задач, що підлягають вирішенню, вибір оптимальної концепції формулювання і підготовки кадрів; оцінюється ділова активність і рівень укомплектованості відділів;
* вибір методу – цей етап в прогнозуванні кадрової роботи обумовлений особливостями структури організації. Методи можуть бути формалізованими і неформалізованими: в першому випадку використовується апарат математичної статистики, у другому – експертні оцінки і пропозиції якісного характеру на основі останніх досягнень науки і практики у сфері підбору, підготовки, розстановки і виховання кадрів;
* прогноз – передбачення основних змін і структурних зрушень в професійно-кваліфікаційному і соціально-демографічному складі кадрів, організації і проведенні кадрової роботи на виробництві.

Визначення потреби в кадрах ведеться окремо для груп персоналу, тобто прогноз чисельності здійснюється для кожної категорії працюючих. Прогнозуючи потребу в окремій категорії працівників необхідно враховувати:

* продуктивність праці або трудомісткість продукції;
* ринкову вартість або ціну виробленої продукції;
* рівень кваліфікації, використовувану технологію;
* організацію виробництва.

Вихідними даними для планування чисельності працівників зазвичай служать обсяги виробництва, трудомісткість виробничої програми, штатні розписи, норми обслуговування, баланси робочого часу одного середньооблікового працівника, графіки змінності.

Безумовно, частина прогнозу будується на певних припущеннях. Наприклад, вибуття за віком прогнозується досить точно, звільнення з посади через невідповідність або на навчання прогнозується на нетривалий період, а вибуття за непередбачуваними обставинами позначається умовною цифрою.

*Принципи планування чисельності і складу працівників*

В рамках кадрового планування, спираючись на вірогідний прогноз, даються відповіді на такі питання:

* скільки працівників, якої кваліфікації, коли і де буде необхідно;
* які вимоги висуваються до тих чи інших категорій персоналу (для цього використовуються професійно-кваліфікаційні моделі посад);
* яким чином залучити потрібний і скоротити непотрібний персонал;
* як використовувати кадри у відповідності з їх потенціалом;
* як забезпечити розвиток цього потенціалу, підвищити кваліфікацію;
* як організувати справедливу оплату праці, мотивацію персоналу і вирішити його соціальні проблеми;
* яких витрат потребують вжиті заходи

Процес планування передбачає п’ять основних етапів:

* оцінювання наявності персоналу;
* оцінювання майбутньої потреби в персоналі;
* розробка програми задоволення майбутніх потреб;
* визначення необхідних витрат, оцінювання задоволення потреб.

Зазвичай планування персоналу здійснюється за такими стадіями:

* підготовча (профорієнтація, профвідбір, професійна підготовка);
* розподільна (набір, відбір і розстановка кадрів);
* адаптаційна.

Процес планування здійснюється з врахуванням ряду принципів.

* Участь максимального числа співробітників організації в роботі над планом вже на ранніх етапах його складання (основний принцип). Якщо мова йде про соціальні заходи, цей принцип є безумовним, в інших випадках його використання є бажаним.
* Неперервність обумовлена необхідністю постійної роботи з кадрами, супроводження їх руху, розвитку і т. д. Тому кадрове планування розглядається не як поодинокий акт, а як регулярно повторюваний процес.
* Наступність вимагає, щоб всі поточні плани розроблялись з урахуванням того, що вони послужать основою складання майбутніх. І одночасно базувались на результатах виконання попередніх.
* Гнучкість передбачає можливість змінювати прийняті кадрові рішення відповідно до обставин, що змінюються. Для цього в плані закладаються так звані «подушки», які при необхідності в певних межах забезпечують свободу маневру.
* Узгодження планів шляхом їх координації та інтеграції, що викликається єдністю і взаємопов’язаністю окремих частин організації. Координація здійснюється по горизонталі, тобто між підрозділами одного рівня, а інтеграція – по вертикалі (між вище- і нижчестоящими). Вони необхідні, оскільки часто одна і та ж робота може виконуватись різними підрозділами, у зв’язку з чим у них з’являються посади, що дублюють одна одну.

• Відповідність вимогам трудового законодавства. Наприклад, потребу в працівниках не можна точно визначити без урахування того, що окремі їх категорії мають право на скорочений робочий час, надання додаткових і навчальних відпусток тощо.

• Врахування індивідуальної і колективної психології працівників. Без цього важко планувати кар’єру, підвищення кваліфікації, внутрішні переміщення людей тощо.

• Створення необхідних умов для виконання плану. Скажімо, план з підвищення кваліфікації так і залишиться на папері, якщо його не підкріпити організацією навчального центру, складанням програм, встановленням контактів з навчальними закладами.

• Максимальне розкриття здібностей працівників.

• Врахування економічних і соціальних наслідків кадрових рішень, що приймаються в фірмі.

*Етапи формування трудового колективу*

Персонал організації формується шляхом узгодження інтересів організації і персоналу, з умовою досягнення цілей розвитку організації при задоволенні потреб працівників. Робота з формування кадрового складу передбачає системний підхід до реалізації декількох етапів, здійснюваних в рамках формування персоналу організації.

* Набір персоналу:
* залучення персоналу:
* визначення джерел залучення персоналу;
* вибір методів залучення персоналу;
* забезпечення привабливості пропонованих вакансій;
* наймання персоналу:
* визначення характеру роботи, вимог робочого місця та посади;
* встановлення мінімальних вимог до кандидатів, залежно від вакантних посад.
* Відбір персоналу:
* комплексне оцінювання кандидатів за рейтингом і формування кінцевого списку;
* створення кадрової комісії з вибору кандидатури на вакантну посаду.
* підбір і розстановка персоналу:
* зіставлення ділових і особистісних якостей працівника з якостями, що їх вимагає дане робоче місце або посада;
* формування трудових колективів з урахуванням соціально-психологічних аспектів сумісності співробітників.

Кожен з цих етапів містить безліч дій, в результаті яких повинен з’явитись необхідний контингент працівників з оптимальними професіональними можливостями і особистісними якостями, необхідними для того, щоб допомогти організації досягти її цілей з урахуванням особистих побажань працівників і їх планової кар’єри.

*Залучення персоналу*

Основною задачею при наймі персоналу є задоволення попиту на працівників в якісному і кількісному складі, тобто, постає питання залучення і відбору осіб в необхідній кількості та наділених потрібними якостями. Наймати нового співробітника чи вибирати з наявних членів трудового колективу – цей вибір роблять під впливом таких факторів:

* важливість, унікальність роботи;
* наявність кадрового резерву і програми розвитку персоналу;
* фінансові можливості компанії;
* особливості кадрової політики.

Перш ніж набирати нових співробітників, важливо визначитись в дійсній необхідності заповнення вакансії. Можливо, що внесення змін в посадову інструкцію, перерозподіл обов’язків існуючих співробітників, використання суміщення посад буде більш вигідним. Процес набору персоналу вимагає величезних затрат, а помилки при призначеннях на посаду роблять їх ще більшими. В той же час, вибір успішних співробітників підвищує прибутковість роботи і престиж фірми, знижує плинність кадрів.

Залучення персоналу – захід з наймання персоналу з метою задоволення в перспективі потреби організації в кадрах за рахунок внутрішніх і зовнішніх джерел. Даний вид діяльності традиційно починається з ринку праці, але ним не обмежується.

 «Пошук і відбір персоналу» виділяє сім етапів в процесі залучення і відбору персоналу . Цей підхід охоплює:

* Визначення потреб у працівниках і критеріїв оцінювання варіантів вирішення проблеми;
* Вироблення філософії і стратегії залучення персоналу, що узгоджуються з загально-організаційною стратегією;
* Отримання точної інформації про те, які вимоги до працівника висуває вакантна посада, встановлення кваліфікаційних вимог, необхідних для успішного виконання роботи, і на основі цього визначення переліку вимог до майбутніх співробітників визначення особистісних і ділових якостей, необхідних для ефективного виконання роботи;
* Розробка сукупності процедур, форм документів, складання письмових правил набору персоналу, вибір методів роботи з претендентами, визначення рівня їх майбутньої оплати праці, способів мотивації і перспектив службового росту;
* Пошук можливих джерел кадрового поповнення й адекватних методів залучення відповідних кандидатів, вибір конкретного варіанта залучення (час, форма залучення, ринки праці);
* Здійснення практичних дій з набору і відбору персоналу, організація процесу створення резерву кандидатів на всі вільні посади, визначення відповідних методів підбору кадрів, що дозволяють найкраще оцінити придатність кандидатів до роботи на даній посаді.
* Забезпечення найкращих умов для адаптації нових працівників до роботи в організації.

Під час набору співробітників для роботи з конфіденційною інформацією важливо не тільки визначити шляхи пошуку кандидатів, але й встановити правове

обґрунтування тих обмежень щодо володіння та використання інформації, які неминуче стосуватимуться даних співробітників.

Починаючи роботу з залучення персоналу необхідно визначити:

* цільові групи, з якими будуть здійснюватись контакти;
* методи встановлення контактів;
* місця, де слід шукати підходящих кандидатів;
* способи стимулювання подачі заяв.

Забезпечення привабливості вакансій будується на визначенні ймовірних мотивів кандидатів. На основі аналізу недоліків і переваг пропонуються заходи підвищення привабливості вакансій.

Можливість швидкого росту, просування по службі. Організації, що розвиваються динамічно, часто дають унікальну можливість зробити швидку кар’єру (що передбачає подальше швидке зростання зарплати).

Можливість самостійної роботи, без жорсткого контролю зі сторони керівництва. Теплі, дружні відносини. Для багатьох людей велику привабливість має клімат командної роботи, коли кожен працівник розуміє, який його вклад в загальну справу, коли він бачить, що успіх загальної справи залежить від зусиль всіх працівників.

Додаткові пільги, якщо немає можливості запропонувати високий рівень оплати. Слід визначити, які додаткові пільги можуть бути запропоновані для залучення висококваліфікованих кандидатів. Це можуть бути:

* організація безкоштовного харчування або оплата харчування;
* надання автомобіля від компанії або грошові компенсації для працівників, які користуються власним автомобілем;
* оплата мобільного телефону;
* медичне страхування за рахунок компанії;
* розпродажі для працівників компанії. Наприклад, деякі торгові компанії влаштовують розпродажі відремонтованої некондиційної техніки для своїх співробітників.

*Джерела залучення персоналу*

Декілька моделей набору персоналу.

* Опора на власні кадри. Означає внутрішнє просування зацікавлених працівників, орієнтованих на цінності організації і відданих їй. Поповнення персоналу здійснюється тільки за рахунок інтелектуальних молодих спеціалістів. Це забезпечує високу стабільність колективу, низьку плинність, задоволеність людей своїм становищем. За рахунок зовнішніх джерел робочої сили заповнюються посади, які не потребують високої кваліфікації і знання особливостей фірми. Вакантні ключові, керівні посади, що потребують високої кваліфікації, заповнюються за рахунок внутрішнього ринку праці, на основі планомірного розвитку і просування персоналу. Головний фактор мотивації – кар’єра.
* Набір кадрів всіх рівнів поза організацією. Це забезпечує високий інтелектуальний потенціал, але прихильність до професії, а не до організації. Головний фактор мотивації тут – нагорода за індивідуальні результати.
* Поєднання ядра постійних і тимчасово залучених працівників характерно для організації з сезонним і нерівномірним завантаженням. Постійне залучення молодих спеціалістів на всі посади, оплата за індивідуальні результати і кваліфікацію. Така модель властива фірмам, що діють у сфері високих технологій на вістрі науково-технічного прогресу.

Спираючись на дані моделі, джерела залучення персоналу можна розділити на зовнішні і внутрішні. До зовнішніх джерел відносять біржі праці, центри зайнятості населення, навчальні заклади різних рівнів акредитації.

Внутрішні джерела залучення персоналу утворюються за рахунок кадрового резерву; поєднання функцій різних посад і переміщення співробітників в рамках одного або кількох підрозділів; перерозподіл обов’язків і наділення співробітника новими функціями, які він буде виконувати в рамках попереднього робочого місця; зростання кваліфікації та рівня освіти персоналу й переміщення співробітників на більш високий ієрархічний рівень організації. І ті, й інші джерела мають свої переваги та недоліки. Перевагами найму зі сторони вважаються:

* порівняна легкість і широкі можливості вибору;
* поява нових ідей про розвиток організації, які вони з собою приносять;
* зниження загальної потреби в кадрах за рахунок залучення додаткових людей;
* відсутність контактів і зобов’язань всередині організації;
* можливість порівняно швидко завоювати авторитет;
* відносно невеликі затрати на навчання.

До недоліків відносять:

* високі витрати;
* погіршення морально-психологічного клімату внаслідок можливих конфліктів між новачками і старожилами;
* високий ступінь ризику через незнання людини, погане знання ним організації і потреба в довгому періоді адаптації.

В цілому зовнішній найм більш придатний для укомплектування низових або вищих посад (на них запрошуються унікальні спеціалісти, яких сама фірма часто «виростити» не в змозі).

Переваги залучення своїх працівників полягають у:

* наданні людям перспектив службового зростання, які підвищують їх задоволеність роботою, віру в себе, що є стимулювальним фактором;
* зберіганні основного складу при скороченні штатів і швидкому заповненні вакансій при звільненні посад;
* хорошому знанні претендентами організації та популярності їх самих, що полегшує адаптацію до нових умов і вимог;
* зниженні плинності кадрів;
* забезпеченні прозорості кадрової політики;
* полегшенні цілеспрямованого підвищення кваліфікації.

З економічної точки зору доцільніше брати підготовлених працівників, але вчити «з нуля» легше, ніж перевчати. В цілому внутрішнє залучення кадрів вважається кращим, але воно також має свої недоліки, до яких відносять:

* обмежений вибір кандидатур;
* необхідність додаткових витрат на перенавчання;
* напруженість в колективі внаслідок зростання внутрішньої конкуренції;
* можливість просувати «потрібних людей»;
* зниження активності співробітників, які залишились «за бортом»;
* збереження загальної потреби в робочій силі.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

При плануванні роботи з персоналом необхідно спиратись на реально існуючі особливості політичної, соціальної та демографічної ситуацій, які тісно пов’язані з балансом трудових ресурсів

**2. Методи залучення персоналу**

Наведемо найбільш поширені методи залучення персоналу, які зустрічаються в сучасних умовах.

* Пошук або підготовка за рахунок коштів організації в навчальних закладах. Сьогодні все більше компаній звертають увагу на випускників передусім через те, що відбувається адаптація системи навчання до потреб ринку. Організації готові ростити для себе кадри з числа молодих фахівців, що поступово пізнають всі етапи виробництва «з нуля». Перевагою тут є приплив свіжих ідей, «незіпсованість» кандидатів, їх не потрібно «ламати», а достатньо створити сприятливі умови для зростання. А недолік в тому, що необхідно більше часу на входження фахівця на посаду в силу недостатності професійного досвіду.
* У конкурентів. Консультанти з найму персоналу знаходять претендентів, спираючись на особисті контакти, бази даних і ін.
* В державних центрах зайнятості. Цей метод дозволяє вести сфокусований пошук кандидатів за відсутності фінансових витрат, але, в основному пропонує осіб масових професій з середньою і низькою кваліфікацією.
* У приватних агентствах з набору персоналу. При звертанні в агентства успіх підбору залежить від того, наскільки чітко сформульовані вимоги до кандидатів, наскільки правильно їх розуміє менеджер агентства, що працює з компанієюзамовником, від його оперативності в роботі. І ще один не менш важливий момент: послуги агентств платні.
* Розміщення оголошень у зовнішніх ЗМІ. Цілі рекламного оголошення: привернути увагу підходящих кандидатур, зацікавити їх організацією і пропонованою роботою, отримати потрібний результат при мінімальних затратах. В даному випадку багато залежить від тиражу, періодичності виходу, системи розповсюдження, іміджу видання.

Оголошення у пресі повинно бути:

* помітним (пусті місця, виділення ключових фраз), коротким, добре написаним;
* містити реальну інформацію про фірму і посаду (не можна допускати переоцінки), але не бути перевантаженим відомостями;

не суперечити законодавству і не містити дискримінаційних моментів;

* стимулювати підходящих людей до подачі заяв («телефонуйте зараз!»);
* перешкоджати їх подачі небажаними особами (інакше багато часу піде на відсіювання претендентів).
* Офіційна інформація у внутрішніх ЗМІ (багатотиражка, спеціальні стенди, дошки оголошень). Можливі як переміщення своїх співробітників, так і приведення ними своїх знайомих.
* Залучення співробітників організації. Виправдано для заповнення вакантних місць керівників середнього і вищого рівня. Вакансії з’являються внаслідок ротації персоналу або введення нових посад в міру розвитку компанії. В цих умовах керівництво звертає свою увагу на вже працюючих в організації співробітників. Цей метод не потребує фінансових витрат, сприяє укріпленню відданості персоналу компанії, кандидатам не потрібно інтегруватись в організацію. Проте такий прийом обмежує вибір, не дає припливу свіжих сил, сприяє виникненню місництва керівників підрозділів, які будуть прагнути зберегти свої найкращі кадри для себе або позбавитись від небажаних.
* Залучення кандидатів за рекомендацією своїх співробітників. Метод використовується для заповнення посад рядових фахівців і набору робітників. Він не потребує фінансових витрат, забезпечує високий ступінь сумісності знову прийнятого персоналу з компанією за рахунок його тісних контактів з уже працюючими фахівцями. Однак рядові співробітники, які рекомендують кандидатів, не є професіоналами в підборі персоналу, можуть не знати посадових обов’язків вакансії, що не дозволяє підбирати персонал високого професійного рівня.
* Паблісіті. Являє собою безкоштовну або платну (але не за рекламними розцінками) статтю про організацію і про переваги роботи в ній, яка готується керівництвом або службою персоналу.

Необхідно фіксувати кількість людей, що відгукнулись на рекламу, і яка ефективність даного способу подачі. Хороше оголошення повинно дати 15-20 відгуків, із яких можна відібрати 5-7 людей. Якщо в результаті рекламної компанії претендентів мало або немає зовсім, потрібно давати повторне оголошення або знижувати заявлені вимоги.

* Пошук в Інтернеті. Є сайти друкованих видань, що висвітлюють ринок праці, сайти кадрових агентств, інтернет-компаній. Багато солідних компаній розміщують вакансії на своїх корпоративних сайтах.

За допомогою Інтернету найбільші західні фірми сьогодні набирають до чверті необхідних їм співробітників. Перевагами Інтернету як інструмент вирішення кадрових проблем можна вважати:

* зниження затрат часу і засобів на залучення персоналу;
* географічну широту контактів;
* надання можливостей широкого взаємного спілкування роботодавця та працівників;
* залучення осіб, зацікавлених в роботі саме в даній корпорації;
* можливість ведення діалогу в реальному режимі часу з претендентами, які знаходяться в будь-якій точці світу.

Але остаточне оцінювання кандидата можливе, безумовно, лише при особистому контакті. До того ж, при використанні Інтернету потрібно бути готовим до напливу кандидатів і великої кількості резюме, на обробку яких потрібна маса часу.

* Організація презентацій організації. На них, як правило, приходять випадкові перехожі або особи, які живуть недалеко, зазвичай з числа тих, хто шукає додаткові заробітки.
* Участь у ярмарках вакансій. Вони зазвичай організовуються місцевою владою. В основному для працевлаштування людей масових професій, які хочуть знайти або змінити роботу.
* Проведення свят і фестивалів. Останні призначені для привертання уваги висококваліфікованих працівників, які цікавляться саме даною організацією.
* Адресна доставка оголошень через пошту.
* Залучення персоналу стимулюється шляхом формування сприятливого іміджу фірми. На підприємстві завжди повинен бути резерв кандидатів на всі посади, з яких організація відбирає найбільш підходящих.
* Очікування осіб, які навмання пропонують свої послуги. Прочитавши оголошення про якусь вакансію, вони пропонують себе просто так, на всякий випадок, без оголошення посади, на яку претендують. Витрати методу мінімальні, як і вірогідність того, що в даний момент часу хтось з таких кандидатів буде затребуваний компанією.

Для успішного пошуку слід використовувати, як правило, декілька методів, що сприяють скороченню строку підбору, підвищенню якості шуканого персоналу, скороченню фінансових витрат. При використанні декількох методів кількість шукачів, з яких можна буде відібрати висококласних фахівців, також буде більшою.

*Розробка вимог до кандидатів*

Вимоги до кандидатів являють собою набір характеристик, яким повинен володіти фахівець, найбільш підходящий на конкретну вакантну посаду. Процес розробки вимог до кандидатів складається з декількох етапів.

* Отримання точної інформації про те, які вимоги до працівника висуває вакантна посада.
* Встановлення кваліфікаційних вимог, необхідних для успішного виконання роботи.

Визначення особистісних і ділових якостей, необхідних для ефективного виконання роботи.

Особливості конкретної професії, що розкривають специфіку професійної праці і вимог, які висуваються до людини, описуються у стандартизованій формі під назвою професіограма. Вона створюється на основі опису професії, який в свою чергу, відповідає на такі питання:

* в чому вона полягає, чи не виконується ким-небудь ще;
* для чого вона призначена і в якому результаті подано;
* чи можуть існуючі співробітники справитись з нею;
* скільки часу і коштів необхідні на перенавчання;
* наскільки робота необхідна в даний момент і на перспективу;
* які потрібні матеріальні, фінансові і людські ресурси та ін.

Професіограма – це опис системи ознак, що характеризують ту чи іншу професію. Вона містить в собі перелік норм і вимог, які висуваються цією професією або спеціальністю до працівника. Професіограма може містити, наприклад, перелік гігієнічних або психологічних характеристик, яким повинні відповідати представники конкретних професіональних груп. Вона містить опис особливостей професії, трудового процесу, вимог, які висуваються до людини (загальна і спеціальна освіта, стаж, професійні навички та ін.). Професіограма може засновуватись на нормативних документах (інструкціях і положеннях) або на результатах вивчення реальної групи осіб.

Існує два види професіограм.

* Професіокарта (кваліфікаційна карта, карта компетентності) – документ, який має в основі посадові інструкції, містить набір кваліфікаційних і особистісних характеристик ідеального співробітника, що необхідні для роботи у відповідній області.

Зміст про професіокарти:

* офіційна назва професії;
* опис результатів праці;
* опис трудових дій і основних особистісних якостей;
* опис предметних і соціальних умов праці;
* можливості навчання і перелік профільних навчальних закладів.

Професіокарта виконує задачу загальної орієнтації в професії, інструмента відбору кандидатів.

* Повна професіограма з описом виробничо-технічних і соціально-економічних умов діяльності, психологічних якостей, які повинен мати працівник.

Складання професіограми починається з розділу «Загальна характеристика професії і її значення». Він містить короткий опис здійснюваної діяльності, її призначення, ролі, результатів і масштабів, престижу, перспективи у зв’язку з НТП, офіційної назви посади, рівня окладу, можливостей професійного росту. Потім на основі детального вивчення ознак професії, умов праці створюється розділ «Особливості трудового процесу. Виконувана робота». Створюваний в результаті опис посади (її задач, прав, обов’язків і основних функцій) допомагає скласти оголошення про найм, форму заяв, визначити кандидатів на співбесіду, прийняти кінцеве кадрове рішення.

Нарешті, на основі опису роботи створюється розділ «Сукупність вимог, що висуваються до особи, ділових і професійних якостей співробітника». У керівників мова йде про якості, необхідні для успішного управління. Вимоги до працівника будуються на основі опису робочого місця (посади). Потрібно відрізняти якості, необхідні при прийомі на роботу, від якостей, які можна швидко отримати. На вимоги організації впливають традиції, ситуація на ринку праці, терміновість. Завищення вимог збільшує час на пошук співробітника, відлякує претендентів, в той час як їх відсутність веде до помилок. Людина, яка відповідає висунутим до неї організацією і посадою (робочим місцем) вимогам, вважається професіонально придатною.

*Методи відбору персоналу*

Наступний етап формування персоналу організації – визначення підходящих методів відбору кадрів, які дозволяють найкраще оцінити придатність кандидатів до роботи.

Відбір персоналу – це процес вивчення психологічних і професійних якостей працівника з метою встановлення його придатності для виконання обов’язків на певному робочому місці або посаді і вибору з сукупності претендентів найбільш придатного з урахуванням відповідності його кваліфікації, спеціальності, особистих якостей і здібностей характеру діяльності, інтересам організації і його самого.

Це процес раціонального вибору тих, хто найкращим чином відповідає вимогам і придатності для виконання обов’язків на робочому місці або посаді. Крім того, цілями відбору є:

* найм працівників, що мають свіжі ідеї;
* залучення людей для перспективної роботи;
* звільнення.

Ефективність і неупередженість відбору персоналу забезпечується наявністю попередньо сформульованих принципів і критеріїв. Процедура комплексна, відповідні заходи проводяться кадровими спеціалістами з необхідною підготовкою.

До прийняття організацією рішення про прийом на роботу кандидат повинен пройти декілька ступенів відбору. Комплекс використовуваних методів відбору може охоплювати:

* завчасний відбір (аналіз інформації про кандидата, що міститься в наданій документації: резюме стандартної форми, диплом, рекомендації і ін.);
* збір інформації про кандидата (від інших людей);
* заповнення бланка заяви і анкети;
* попередню відбіркову бесіду (з тими, що пройшли відбір за документами);
* групові методи відбору;
* особистісні запитальники і тести (в тому числі психологічні тести і тести професійних здібностей);
* співбесіда-інтерв’ю;
* медичний огляд;
* прийняття рішення.

Принципи відбору персоналу:

* орієнтація на сильні, а не на слабкі сторони людей;
* пошук не ідеальних кандидатів, яких в природі не існує, а найбільш перспективних і відповідних для даної посади (він припиняється, якщо декілька людей так і не змогли задовольнити висунуті вимоги, бо, скоріш за все, останні завищені);
* відмова в прийомі нових працівників незалежно від кваліфікації і особистих якостей, якщо потреба в них відсутня;
* забезпечення відповідності індивідуальних якостей претендентів (освіти, стажу, досвіду, а в ряді випадків – статі, віку, здоров’я, психологічного стану) вимогам посади;
* залучення найбільш кваліфікованих кадрів (хороший фахівець, скільки б йому не платили, завжди обходиться дешевше, ніж поганий), але не більш високої

кваліфікації, ніж потрібно;

* перевищення очікуваного ефекту над витратами;
* збереження сприятливого психологічного клімату;
* задоволення очікувань прийнятих на роботу співробітників.

У багатьох випадках підбір співробітників здійснюється переважно на основі їх освіти. Але це далеко не завжди дозволяє досягнути потрібного результату. Рівень, характер і якість освіти повинні враховуватись поряд з іншими вимогами, що висуваються конкретною посадою, роботою. Важливими критеріями є: соціальний статус і вік кандидата, його професійний досвід, професійно важливі якості і особистісні особливості. Щоб вибір був правильним, необхідно, насамперед, враховувати обґрунтованість прийнятих критеріїв. Під обґрунтованістю критерію розуміється те, з якою точністю одержувана з його допомогою оцінка відповідає дійсній характеристиці кандидата. Критерії відбору персоналу повинні відповідати змісту роботи і вимогам до посади. Забезпечуючи достовірність і стійкість результатів, необхідно враховувати всі головні характеристики, важливі для ефективної роботи.

*Підбір і розстановка персоналу*

Підбір і розстановка персоналу в організації, будучи безпосереднім вираженням розподілу і кооперації праці, створює виробничий колектив. Відбираючи кандидатів, спираються на їх професійні, ділові і особисті якості, формуючи ж трудовий колектив, необхідно мати на увазі ефект поєднання – так звану психологічну сумісність, яка допомагає людям швидко та успішно спрацюватися один з одним, що породжує задоволеність своєю роботою і веде до зростання продуктивності праці. Зупинимось детальніше на технічних моментах підбору і розстановки персоналу. Основна відмінність підбору персоналу від відбору полягає в тому, що в першому випадку порівнюються ділові та особистісні якості працівника з якостями, необхідними на даному робочому місці (посаді), а в останньому виділяється який-небудь кандидат з загального числа претендентів на дану посаду. Підбір і розстановка кадрів основується на принципах відповідності, перспективності, змінюваності. Принцип відповідності означає відповідність моральних та ділових якостей претендентів вимогам посад, які заміщаються.

Принцип перспективності ґрунтується на врахуванні таких умов:

* встановлення вікового цензу для різних категорій посад;
* визначення тривалості періоду роботи на одній посаді, на одній і тій же ділянці роботи;
* можливість зміни професії або спеціальності, організація системного підвищення кваліфікації;
* стан здоров’я.

Принцип змінюваності полягає в тому, що кращому використанню персоналу повинні сприяти внутрішньо-організаційні трудові переміщення. Він спирається на думку, що застій (старіння) кадрів, пов’язаний з довготривалим перебуванням на одній і тій самій посаді, має негативні наслідки для діяльності організації. Отже, необхідні зміни місця працівників у системі розподілу праці, а також зміни місця прикладання праці в рамках організації. Щоб постійне і планомірне оновлення не переходило в плинність кадрів, даний процес повинен базуватись на таких принципах:

* оновлення не повинно сприйматись як метод дискваліфікації працівників, які сумлінно виконують свої обов’язки;
* необхідно враховувати інтереси керівників і фахівців, їх можливості для роботи на інших посадах;
* повинна створюватись можливість використання на нових посадах управлінського досвіду, набутого працівниками на попередньому місці роботи.

*Аналіз професійних та особистісних якостей претендентів*

Фактично, оцінювання при прийомі – це одна з форм попереднього контролю якості людських ресурсів організації.

Психологічні особливості особистості і ставлення до праці та колективу значною мірою визначають поведінку людини в трудовій сфері. Для дослідження професійних і особистісних якостей претендентів, відповідності їх вимогам робочого місця, існує ряд методів і тестів.

Перевірка професійних якостей працівників під час трудової діяльності здійснюється досить часто: при прийомі, при переміщенні, при атестації. Методи здійснення такої перевірки загальновідомі, і вони, природно, припускають наявність критеріїв, стандартів відповідності вимогам, які можуть бути виміряні або оцінені в порівнянні з якостями, що притаманні працівникові. У більшості випадків для перевірки професійних якостей доцільно розробити або застосувати такі існуючі методи перевірки рівня професіоналізму, як виконання перевірочної роботи, зміст якої має відповідати вимогам тарифно-кваліфікаційного довідника, посадової інструкції. Для перевірки рівня кваліфікації працівникові дається завдання, визначається час виконання завдання (за нормами часу) і якість. Рівень знань, теоретичної підготовки перевіряється під час проведення іспиту, опитування за заздалегідь відомими питаннями, що відображають стандарт освіти, який відповідає рівню кваліфікації, що перевіряється. Власне, будь-яку діяльність можливо детермінувати і нормувати, використовуючи, наприклад, методи порівняння, екстраполяції, експертних оцінок, розглянуті раніше. Цей підхід, в принципі, відповідає психодіагностичному методу, названому «тести досягнень», які спрямовані на виявлення ступеня володіння випробовуваним конкретними знаннями, вміннями, навичками.

На стадії прийому широку інформацію про професійні та особистісні якості працівників дає аналіз результатів випробувального терміну. Після закінчення випробувального терміну як експерти можуть бути залучені будь-які працівники, які співпрацювали з новачком, з використанням стандартизованої форми, складеної з урахуванням вимог до проведення соціально-психологічних досліджень. З точки зору методів дослідження особистісних властивостей людини випробувальний термін може розглядатися як аналог природного соціально-психологічного експерименту. У той же час в цей період можуть застосовуватися і лабораторні експерименти, із застосуванням спеціальної апаратури, зі створенням умовних ситуацій (наприклад, шляхом проведення ділових ігор та розгляду ділових ситуацій). При необхідності здійснення коригувальних або навчальних впливів використовуються методи формувальних (навчальних) експериментів. Щоб отримати можливість прогнозувати поведінку людини в широкому класі можливих ситуацій, психологи прагнуть виміряти базисні або універсальні риси. Ці риси належать, як правило, до найбільш загальних структурно-динамічних характеристик стилю діяльності. Риси розуміються як послідовність поведінки, звички або тенденції до повторення поведінкових проявів. Вони ієрархічно організовані, їх верхній рівень утворюють фактори. Фактори мають безліч різноманітних поведінкових проявів, відносно стабільні (постійні в часі при незмінності звичних умов життя), відтворюються в різних дослідженнях і соціально значимі. Іноді чинники називають базисними, або універсальними, рисами. Типології методів визначення особистісних якостей працівників і особливостей рольового розподілу в групі, ставлення працівників групи один до одного досить різноманітні, але найчастіше виділяють такі комплекси методів:

* метод зовнішнього спостереження. Він полягає у навмисному, систематичному, цілеспрямованому та організованому сприйнятті і реєстрації поведінки досліджуваного об’єкта. Метод трудомісткий вимагає значного часу, та спеціальної підготовки;
* метод самоспостереження (інтроспекції) – стратегія отримання емпіричних психологічних даних при спостереженні людини за собою, за власними психічними проявами. Зазвичай висновки, які робить людина на основі самоспостереження, суб’єктивні, неадекватні і можуть використовуватися для аналізу самооцінки і при порівнянні з думкою оточуючих;
* особистісні опитувальники, анкети або тести для діагностики ступеня вираженості в індивіда певних особистісних характерологічних або інших рис (тривожність, фрустрація, самотність, агресивність, емпатія, акцентуації характеру, темперамент, самооцінка). Можна виділити 2 види опитувальників: одновимірні – діагностується одна будь-яка характеристика, і багатовимірні – дають інформацію про цілий ряд різних властивостей особистості. Даний вид дослідження дозволяє визначити такі різні властивості і якості особистості, як темперамент, характер, інтелект, схильність до творчості, мотиви поведінки, ціннісні орієнтації, фактори, що впливають на поведінку і т. п. Оскільки відповіді дає сам опитуваний, одержувані дані містять значний елемент суб’єктивізму; на якість відповідей впливає і психологічний стан опитуваного, і ступінь фактичного знайомства з ситуацією, поведінку в якій пропонується охарактеризувати;
* проективні методи, основані на інтерпретації проекцій випробовуваного на стимулювальний матеріал. Традиційно проектні тести відносять до числа найбільш надійних, однак для багатьох проективних методик принципово важливою виявляється роль психолога-діагноста, його досвід і професіоналізм, що пов’язано з деякою свободою в його інтерпретаціях. Професійний психолог в змозі розпізнати за асоціаціями, що їх викликає у суб’єкта стимулювальний матеріал, особливості його особистості, мотивів, цінностей, роботу підсвідомості. При використанні даних методів присутність досвідченого професіонала в галузі психології обов’язкова;
* соціометрія – метод психологічного дослідження міжособистісних відносин у групі з метою визначення структури взаємовідносин, ролей і статусів членів групи, у т. ч. виявлення неформальних лідерів, психологічної сумісності. Є комплекс тестів для визначення соціально-психологічного клімату в групі, ставлення до лідера, до керівника, для виявлення стилю керівництва;
* методи анкетування, інтерв’ю, бесід, що дозволяють отримати інформацію шляхом відповіді на письмові або усні запитання фахівця. Дані методи широко застосовуються в системі маркетингу, при необхідності виявлення ставлення до праці, наприклад, «Анкета про наявні та бажані повноваження».

Використовуються вони і при різних видах соціологічних досліджень, вимагають участі фахівців для розробки програми дослідження, його організації, проведення та подальшої інтерпретації результатів.

*Особливості відбору співробітників, які допускаються до роботи з конфіденційною інформацією*

Один з найбільш важливих етапів у роботі з персоналом підприємства – процес підбору можливих кандидатів для призначення на посади, пов’язані з конфіденційною інформацією. При підборі кандидатів оцінюється відповідність кожного з них таким основним вимогам:

* за рівнем підготовки та кваліфікації, наявності необхідного досвіду роботи;
* за морально-діловими і особистісними якостями;
* за ступенем відповідальності за прийняті управлінські та виконавські рішення (залежно від займаної посади).

При підборі кандидатів для призначення на посади, пов’язані з конфіденційною інформацією, в обов’язковому порядку враховується рівень кожної конкретної посади з точки зору прийняття та реалізації управлінських рішень, виконання організаторських функцій і завдань повсякденної діяльності підприємства. Виходячи з названих критеріїв, дані посади поділяють на такі групи:

* посади керівників підприємства (керівник підприємства, його філії, представництва);
* посади заступників керівника;
* посади керівників структурних підрозділів;
* посади керівників служб безпеки та їх заступників;
* посади співробітників служб безпеки підприємства;
* посади співробітників підприємства, які здійснюють на постійній основі роботу з конфіденційною інформацією у відповідних структурних підрозділах.

При відборі кандидатів для призначення на перераховані посади додатково враховується обсяг і важливість відомостей конфіденційного характеру, до яких допускаються працівники, що займають ці посади. Організаційні заходи при підборі персоналу, що одержує доступ до конфіденційної інформації, можна розділити на кілька груп:

* проведення ускладнених аналітичних процедур при прийомі і звільнення співробітників;
* документування добровільної згоди особи не розголошувати конфіденційні відомості та дотримуватися правил забезпечення безпеки інформації;
* інструктування і навчання працівників практичним діям із захисту інформації.

У ході попередньої бесіди з оформлюваним на роботу громадянином працівник кадрового органу поряд з уточненням окремих питань анкети, що заповнюється при оформленні матеріалів на допуск до державної таємниці, виявляє відомості, які не передбачені питаннями анкети але викликають інтерес:

* чи мав громадянин за останній рік відношення до секретних робіт, документів і виробів;
* чи давав він зобов’язання щодо нерозголошення відомостей, що становлять державну таємницю;
* чи працював (служив) на режимних об’єктах.

При бесідах і співбесідах з кандидатами на посаду в області захисту інформації переслідуються такі цілі:

* виявити реальну причину бажання кандидата працювати на даній фірмі;
* виявити можливих зловмисників або спробувати побачити слабкості кандидата як людини, які можуть сприяти шпигунству;
* переконатися, що кандидат не приніс з собою конфіденційну інформацію іншої фірми, яку хоче таємно використовувати;
* переконатися в добровільній згоді кандидата дотримуватися правил захисту інформації та мати певні обмеження у професійному та особистому житті.

Працівник кадрового органу також запитує необхідні довідки та документи, знайомить претендента зі змістом договору (контракту) про оформлення допуску до державної таємниці. Особливу увагу секретар-референт повинен звертати на аналіз достовірності та правильності оформлення персональних документів: відповідність прізвищ, імен та по батькові, інших персональних даних, наявність у документах необхідних відміток і записів, ідентичність фотокарток і особи громадянина (на фотографії окуляри, борода, перука – тільки при постійному носінні), відповідність форми бланка документа роками їх використання, відсутність підчисток, незавірених виправлень, спроб заміни аркушів, фотографій і т. п. Усі печатки повинні відповідати назвам тих організацій, які видали документ. Наприклад: трудова книжка повинна відповідати формі, встановленій для того періоду часу, коли вона була видана, або мати напис «дублікат», містити запис про звільнення з останнього місця роботи, завірений печаткою, і т. п. При якихось сумнівах громадянина просять подати дублікати зіпсованих документів, завірити виправлення. Документи, що викликали явний сумнів, повертаються громадянину, і одночасно йому відмовляється у розгляді питання про прийом на роботу. Тільки після ретельного аналізу поданих документів з кандидатами на посаду проводиться співбесіда. Основні особисті якості, які повинен мати потенційний працівник, пов’язаний з конфіденційною інформацією:

* порядність, чесність, принциповість і сумлінність;
* старанність, дисциплінованість;
* емоційна стійкість (самовладання);
* прагнення до успіху і порядок у роботі;
* самоконтроль у вчинках і діях;
* адекватна самооцінка власних можливостей і здібностей;
* помірна схильність до ризику;
* вміння зберігати секрети в будь-яких обставинах і будь-якому стані;
* тренована увага;
* хороша пам’ять, вміння вести порівняльне оцінювання фактів, пропозицій і т. д.

Особисті якості, які не сприяють збереженню секретів:

* емоційний розлад;
* неврівноваженість поведінки;
* розчарування в собі і своїх здібностях;
* відчуження від колег по роботі;
* невдоволення своїм службовим становищем;
* ображене приватне самолюбство;
* вкрай егоїстична поведінка;
* відсутність достатньої розсудливості;
* небажання і нездатність захищати інформацію;
* нечесність;
* фінансова безвідповідальність, бажання отримувати гроші без особливих затрат розумових і фізичних сил;
* вживання наркотиків;
* негативний вплив алкоголю, що приводить до балакучості, необдуманих вчинків, випадкових знайомств і зв’язків тощо.

Після прийняття рішення про призначення кандидата, який найбільш повно задовольняє пропоновані вимоги, на посаду, пов’язану з допуском до конфіденційної інформації, керівник структурного підрозділу, до якого призначено особу, спільно зі службою безпеки підприємства (режимно-секретним підрозділом) організовує проведення інструктажу. У ході інструктажу до відома новопризначеної особи доводяться його посадові обов’язки, положення нормативно-методичних та внутрішніх організаційно-розпорядчих документів, що регламентують питання захисту конфіденційної інформації на підприємстві. І. А. Бородін пропонує такий план інструктивної бесіди перед зарахуванням до штату.

* Обговорення політики Роботодавця щодо конфіденційної інформації:  цього роботодавця;  інших роботодавців.
* Ознайомлення з формою угод про конфіденційну інформацію та обговорення їх з кандидатом на роботу:
* звернення уваги кандидата на серйозність цієї угоди;
* складання списку колишніх винаходів, відкриттів, теоретичних розробок, автором яких є кандидат на роботу.
* Отримання завірених підписом гарантій щодо прав третіх осіб.
* Обговорення можливих обмежень в обов’язках на новому місці роботи:
* розбір системи підпорядкованості;
* ознайомлення з перспективами службового зростання.

Підготовка співробітника до виконання обов’язків за новою посадою здійснюється за планом, який затверджується керівником структурного підрозділу, до якого призначений даний співробітник.

У процесі відбору персоналу виявляються співробітники, які не відповідають вимогам організації, і тоді на порядку денному постає питання про звільнення. Зі співробітниками підприємства, допущеними до конфіденційної інформації, етап звільнення (переведення на посади, не пов’язані з конфіденційною інформацією) займає особливе місце. Після прийняття керівництвом підприємства рішення про звільнення співробітника, допущеного до конфіденційної інформації, або про переведення його на посаду, не пов’язану з доступом до конфіденційної інформації, службою безпеки та кадровим органом підприємства проводиться ряд заходів, спрямованих на запобігання можливого розголошення звільненим співробітником конфіденційної інформації про діяльність підприємства. Основою проведення даних заходів є прийняття від звільненого співробітника письмових зобов’язань про нерозголошення відомостей, які стали йому відомими у період роботи на підприємстві (на конкретній посаді), у встановленому порядку віднесених до комерційної таємниці підприємства.

Ці зобов’язання оформляються у вигляді розписки, яка після її оформлення залишається на підприємстві. У розписці зазначаються прізвище, ім’я, по батькові співробітника та найменування останньої займаної посади; перераховуються відомості конфіденційного характеру, заборонені до розголошення протягом певного терміну, або наводиться посилання на пункти переліку відомостей, віднесених до комерційної таємниці. Згода працівника з умовами нерозголошення перерахованих в розписці відомостей підтверджується підписом співробітника із зазначенням дати. Оформлення розписки здійснюється, як правило, в ході бесіди зі співробітником підприємства представника служби безпеки або режимно-секретного підрозділу. Після оформлення розписки проводиться інструктаж звільненого співробітника про правила його поведінки після звільнення (переведення на іншу роботу) і про недопущення згадки конфіденційних відомостей в ході спілкування з представниками організацій, що є конкурентами даного підприємства. Особливу увагу в ході інструктажу приділяється необхідності збереження в таємниці конфіденційної інформації при спілкуванні з іноземними громадянами (при взаємодії в процесі майбутньої роботи з іноземними організаціями).

Перед звільненням з підприємства (переведенням на роботу, не пов’язану з конфіденційною інформацією) співробітник зобов’язаний повернути в службу безпеки підприємства (режимно-секретний підрозділ) отримані раніше носії конфіденційної інформації (у тому числі накопичувачі на магнітних дисках), номерні металеві печатки, ключі від сейфів і сховищ.

Факт повернення підтверджується відповідними підписами відповідальних посадових осіб у обхідному листі співробітника, що звільняється. Після заповнення обхідного листа співробітникові видається оформлена трудова книжка та інші документи про звільнення. Отримавши трудову книжку і провівши повний розрахунок з підприємством, звільнений співробітник повертає в бюро перепусток (на контрольно-пропускний пункт при вибутті з підприємства) пропуск для проходу на територію і об’єкти підприємства.

*Методи тестування у кадровій роботі*

Більш точно визначити стан кандидата з точки зору його відповідності вимогам, що висуваються до вакантної посади, а також потенціалу розвитку можна за допомогою спеціальних тестів, у тому числі і на професійну придатність і психологічний стан. Актуально використання тестування для діагностики різних якостей і характеристик особистості – темпераменту, аналітичних здібностей, комунікабельності, швидкості реакції, пам’яті, лідерських даних і т. д.

 Найбільш часто використовуються нижченаведені тести.

Тест MMPI університету Міннесоти складається більш ніж з 550 пунктів, дозволяє виробити 10 вимірювань особистості згідно з патологічними категоріями, описаними в психіатрії. Перші чотири шкали дозволяють перевірити щирість і обґрунтованість відповідей випробовуваного, а клінічні шкали відповідають різним категоріям психічних порушень:

* іпохондрії (перебільшена заклопотаність своїм здоров’ям);
* депресії;
* істерії;
* схильності до психопатії;
* коефіцієнт «мужність – жіночність»
* схильності до шизофренії (зміна особистості);
* до параної (систематизоване стійке марення переслідування, ревнощів, винахідництва і т. п.);
* до психастенії (тривожність);
* манії (одержимість хворобливою пристрастю до чого-небудь).

Крім того, визначається співвідношення екстраверсії та інтроверсії. За допомогою опитувальника вдається отримати повну картину або профіль особистості, де кожен показник оцінено в балах. Нормальним вважається профіль, показники якого знаходяться в межах 30-70 балів. Розроблено вітчизняні варіанти цього опитувальника.

Значне поширення в нашій країні отримав багатофакторний опитувальник особистості Р. Б. Кеттелла (тест 16 PF). Опитувальник призначений для виявлення 16 факторів, ідентифікованих Кеттелл для визначення психічного профілю людини за поверхневими особистісними властивостями. Профіль особистості визначається поєднанням бальних значень по парах таких факторів, як:

* замкнутість – товариськість;
* емоційна стійкість – нестійкість;
* підкорюваність – домінантність;
* боязкість – сміливість і т. п.

Тест MPI Айзенка дозволяє визначити ступінь стабільності – нестабільності (нейротизму) нервових процесів суб’єкта і співвідношення екстраверсії – інтроверсії. При інтерпретації результатів вимірювані характеристики визначаються рисами темпераменту, мають тісний зв’язок з фізіологічними особливостями людини. Основний зміст фактора екстраверсія – інтроверсія він трактував як відкритість – закритість суб’єкта зовнішнім впливам. Разом з тим його поведінкові прояви описувалися досить широко: для екстраверсії характерні тяга до нових вражень, до розкутих форм поведінки, підвищена імпульсивність, висока рухова і мовна активність, товариськість, оптимізм; для інтроверсії характерні спрямованість на себе, загальмованість рухів і мови, замкнутість, слабка тяга до нових вражень, переважання поганого настрою. Шкала нейротизму відображає різні характеристики емоційної сфери: емоційну лабільність, чутливість і тривожність.

Шкала LOG Pommepa дозволяє встановити так званий «локус контролю», тобто спрямованість суб’єктивної оцінки: чому схильна приписувати людина причини своїх досягнень і невдач – зовнішнім, незалежним від неї обставинам, або власним, внутрішнім чинникам.

Тест Томаса – на визначення стилю поведінки в конфлікті.

Найбільш відомі з тестів, заснованих на використанні проективних методів, – це «чорнильні плями Роршаха», тест тематичної апперцепції (усвідомленого сприйняття) Маррея. Необхідно пам’ятати, що для роботи з використанням цих методів потрібно неодмінна участь кваліфікованого психолога. Інтерпретуючи результати дослідження, необхідно дотримуватись певної обережності, тобто тестування має розглядатися тільки як допоміжний засіб у визначенні якостей людини. Використання тестів можливе тільки в пакетах, коли дані, отримані одним способом, перевіряються при застосуванні іншого, тому що багато пунктів мають дуже загальний характер, випробовуваний часто підпадає під вплив авторитету вченого, який розробляє або застосовує тест, і відповідає на питання не щиро, а так, як, на його думку, хотілося б вченому. На результати тестування впливають втома і занепокоєння, деякі тести вторгаються в особисте життя випробовуваного. Доступність тестового матеріалу дозволяє ознайомитися з ним заздалегідь і відповідати, фальсифікуючи результати. Окрему групу утворюють профорієнтаційні тести: якщо для використання особистісних опитувальників на етапі профвідбору або переміщення працівника потрібне попереднє уявлення про необхідні якості і властивості, а особистісні опитувальники допомагають встановити їх наявність, то профорієнтаційні тести допомагають визначити сферу діяльності, до якої опитуваний має схильність. Американський дослідник Джон Л. Голланд встановив, що вибір професії є вираженням особистості, а досягнення людини залежать від відповідності між його особистістю та обставинами роботи (змістом, характером та умовами праці). На його думку, кожна людина, певною мірою, належить до одного з 6 типів особистості:

* реалістичний – надає перевагу діяльності, пов’язаній з маніпуляціями інструментами та механізмами;
* дослідний – надає перевагу аналітичній роботі, допитливий, методичний, точний;
* артистичний – експресивний, нонконформіст, оригінальний, внутрішньо зосереджений;
* соціальний – полюбляє роботу з людьми, допомагати іншим, але не систематичну діяльність;
* підприємницький – полюбляє впливати на інших для досягнення цілей;
* конвенціальний – полюбляє систематичне маніпулювання даними, записами; репродукування матеріалів.

Зазвичай один тип домінує, але людина, пристосовуючись і змінюючи спектр використовуваних стратегій, може досить успішно займатися видами діяльності, передбаченими для двох або трьох типів особистості. При цьому для вибору кар’єри, сфери діяльності важлива близькість домінуючого і додаткового типів. Наведений у тесті порядок типів особистості не випадковий: він показує поступовий перехід якостей від типу до типу. Сусідні типи в цьому списку ближче один до одного, варіанти успішної кар’єри за ними легше вибрати тим, у кого домінуючий і допоміжний типи граничні, а не далекі. Таким чином, вважається, що більш широкий діапазон видів діяльності, в яких людина буде відчувати себе комфортно і зможе досягти успіху, у людей типу соціальний підприємницький або соціальний-артистичний, ніж соціальний-реалістичний. Диференційно-діагностичний опитувальник Е. А. Климова дозволяє виявити орієнтацію за 5 напрямками діяльності. На основі вибору з 20 пар тверджень робиться висновок про орієнтацію на такі види, сфери чи об’єкти діяльності, як природа, техніка, людина, знакова техніка (знаковий образ), художній образ. Здійснюючи дослідження особистісних якостей співробітників служб інформаційної безпеки, є прямий резон використовувати Тест К. Леонгарда, який спрямований на виявлення акцентуації характеру. Модифікація даної методики виконана С. Шмішеком. Методика призначена для виявлення різних рівнів акцентування особистості. Акцентуації розглядаються як крайні варіанти норми, а не патології. На думку Леонгарда, акцентованим особистостям властива готовність до особливої, тобто як соціально-позитивної, так і соціально-негативної поведінки.

Дослідження особистості проводиться за шкалами: гіпертимність, ригідність, емотивність, педантичність, тривожність, циклотимність, демонстративність, збудливість, дістімність, екзальтованість.

 Дуже інформативний тест «Визначення схильності до відхилень».

Шкали: схильність до подолання норм і правил, схильність до адиктивної (залежної) поведінки, схильність до самопошкоджувальної і саморуйнівної поведінки, схильність до агресії та насильства, вольовий контроль емоційних реакцій, схильності до деліквентної (антигромадської протиправної) поведінки. Дана методика діагностики схильності до відхилень (СДВ) є стандартизованим тест-опитувальником, призначеним для вимірювання готовності (схильності) до реалізації різних форм поведінки, що відхиляється, і являє собою набір спеціалізованих психо-діагностичних шкал. Методика передбачає врахування і корекцію установки на соціально бажані відповіді випробовуваних. Шкали опитувальника діляться на змістові та службову. Змістовні шкали спрямовані на вимірювання психологічного змісту комплексу пов’язаних між собою форм девіантної поведінки, тобто соціальних та особистісних установок, що стоять за цими поведінковими проявами. Службова шкала призначена для вимірювання схильності випробовуваного давати про себе соціально схвалювану інформацію, оцінювання достовірності результатів опитувальника в цілому, а також для корекції результатів за змістовними шкалами залежно від вираженості установки випробуваного на соціально бажані відповіді.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Зазвичай один тип домінує, але людина, пристосовуючись і змінюючи спектр використовуваних стратегій, може досить успішно займатися видами діяльності, передбаченими для двох або трьох типів особистості. При цьому для вибору кар’єри, сфери діяльності важлива близькість домінуючого і додаткового типів.

**ВИСНОВКИ З ТЕМИ**

Найчастіше кадрове планування розуміється як процес забезпечення організації необхідною кількістю кваліфікованого персоналу, прийнятого на відповідні посади в потрібний час. Очевидно, що ключовими моментами є саме якісна і кількісна відповідність персоналу фронту робіт. Оскільки реалізація цього тезису залежить від багатьох компонентів, то і визначення кадрового планування стає набагато ширшим. В загальному вигляді кадрове планування – це діяльність організації, спрямована на підготовку кадрів, забезпечення пропорційного і динамічного розвитку персоналу, розрахунок професійно-кваліфікованої структури кадрів, визначення загальної і додаткової потреби в них, контроль використання персоналу.

**ТЕМА 5. ПРОМИСЛОВЕ ШПИГУНСТВО В ПІДПРИЄМНИЦЬКІЙ ДІЯЛЬНОСТІ**

**ПЛАН ЛЕКЦІЇ:**

1. Поняття промислове шпигунство

2. Комерційна таємниця

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

1.Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. –Львів : Видавництво Львівської політехніки, 2015. –256 с.

2.Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації -Харків: ХНУРЕ, 2004 -368 с.

3.Лагун А. Е. Криптографічні системи та протоколи: нав. посібник / А. Е. Лагун. –Львів : Видавництво Львівської політехніки, 2013. –96 с

4. Інформатика в юридичній діяльності / Кудінов В.А., Хахановський В.Г., Пакриш О.Є. та ін. за заг. редакцією В.А. Кудінова. – К.: Нац. акад. внутр. справ, 2016. – 256 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2014.

**МЕТА ЛЕКЦІЇ:**

Познайомити студентів з основними поняттями промислове шпигунство, правовою базою та комерційною таємницею.

**ВСТУП**

Промислове (комерційне) шпигунство – один з видів недобросовісної конкуренції, який є досить поширеним у сучасному світі. Промислове шпигунство є діяльністю із незаконного добування відомостей, що становлять комерційну цінність.

**1. Поняття промислове шпигунство**

Відповідно до ст. 16 Закону України «Про захист від недобросовісної

конкуренції» неправомірним збиранням комерційної інформації вважається збирання протиправним способом відомостей, що становлять відповідно до законодавства України комерційну таємницю, якщо це завдало чи могло завдати шкоди суб’єкту господарювання.

Комерційною таємницею, в свою чергу, є інформація технічного, організаційного, комерційного, виробничого та іншого характеру, яка є невідомою та не є легкодоступною для осіб, що мають справу з таким видом інформації.

Найчастіше метою промислового шпигунства стає інформація саме такого виду: будь-які унікальні (нові) розробки і нові технології, які можуть становити об’єкти інтелектуальної власності, ноу-хау, інноваційні ідеї, фінансові показники і т. п.

Промислове шпигунство має давню історію і безліч «пристойних» назв, серед яких: економічна розвідка, конкурентна розвідка, ділова (бізнес) розвідка. Однак, безперечно, промислове шпигунство – це завжди таємне (незаконне) збирання будь-якої інформації, що становить комерційну, службову, промислову таємницю, мета якого – випередити конкурента, захопити ринок, зміцнити своє становище на ринку і т. д.

Необхідно відзначити, що збір інформації про конкурента може бути здійснений і легальними способами за допомогою відкритих реєстрів, доступної публічної інформації. Якщо говорити про термін «промислове шпигунство», то в такому випадку мова йде про збір інформації саме незаконними методами.

 Промислове шпигунство може здійснюватися різними шляхами:

*прослуховування розмов, перехоплення комп’ютерної інформації, прихована фото- та відеозйомка, підкуп працівника і т. п.*

Захиститися від промислового шпигунства досить складно, особливо в нашій країні, оскільки українські компанії часто не готові витрачати значні кошти на технічні системи захисту інформації. Однак без попередження випадків промислового шпигунства не обійтися, мабуть, жодному підприємству, що володіє будь-якою інформацією, яка може являти собою комерційну таємницю.

Серед способів профілактики промислового шпигунства можна виділити наступні:

– ефективна кадрова політика;

– укладання з працівниками угод про нерозголошення комерційної

таємниці;

– прорахунок заздалегідь усіх можливих ризиків витоку інформації;

– технічні засоби захисту інформації;

– системи стеження і контролю.

Ефективна кадрова політика, як би піднесено це не звучало, є чи не найважливішим способом запобігання витоку інформації. Така політика включає перевірку працівників, проведення співбесід, складання внутрішніх нормативних документів щодо режиму конфіденційності.

Укладання з працівниками угод про нерозголошення комерційної таємниці (конфіденційної інформації) також досить важливий фактор профілактики витоку інформації. Однак у таких угодах дуже бажано вказувати конкретний перелік інформації, що є конфіденційною і не підлягає розголошенню.

Ідентифікуючи найбільш цінні дані, можна визначити, кому і з якою метою вони можуть знадобитися, що дасть розуміння шляхів можливих атак (хакінг, підкуп відповідальних працівників). Крім того, доцільно закріплювати в таких угодах цивільно-правову відповідальність працівника за розголошення такої інформації (в разі доведення його провини) за понесені компанією збитки.

У трудових договорах також доцільно вказати, що розголошення комерційної таємниці є порушенням трудової дисципліни, закріпивши таким чином дисциплінарну відповідальність (догана, звільнення).

Завчасний прорахунок всіх можливих ризиків витоку інформації дозволить передбачити можливі прогалини в діяльності суб’єктів господарювання. З цією метою зазвичай складається список інформації, яка може становити комерційну таємницю. Ідентифікуючи найбільш цінні дані, можна визначити, кому і з якою метою вони можуть знадобитися, що дасть розуміння шляхів можливих атак (хакінг, підкуп відповідальних працівників).

Технічні способи захисту інформації є дуже важливим фактором у профілактиці промислового шпигунства. Необхідно не тільки захищатися від можливих атак, а й належним чином зберігати цінну інформацію: обмежувати доступ до неї не тільки третім особам, а й співробітникам; зберігати особливо цінну інформацію в закодованому вигляді; не передавати цінну інформацію жодними засобами зв’язку.

На сьогоднішній день профілактика промислового шпигунства дуже ускладнюється зважаючи на постійний розвиток інформаційних технологій і доступності Інтернету. Хакерські атаки на різні інформаційні системи набули сьогодні воістину колосальних обсягів. Протистояти і захищатися від нових технологій (пристроїв), спрямованих на зняття інформації, багатьом компаніям просто не по кишені.

*Оперативне правове реагування*

При підозрі на найменші загрози витоку інформації реагувати бажано дуже оперативно.

Звичайно ж, в першу чергу при підозрі витоку інформації будь-яким шляхом необхідно встановити джерело такого витоку, якщо це технічно можливо. У будь-якому випадку, важливо розуміти, яким чином стався такий витік: через співробітників чи через засоби зв’язку. У разі розуміння або підозри, що витік (крадіжка) інформації стався з вини співробітника, необхідно вжити заходів щодо тимчасового відсторонення такого(-их) співробітника(-ів) і щодо проведення внутрішнього розслідування.

Для виявлення того (тих) співробітника(-ів), хто може бути винен у витоку, необхідно визначити коло осіб, яким була доступна така інформація і кому вона була передана.

Якщо витік (крадіжка) інформації може загрожувати інтересам третіх осіб, необхідно в терміновому порядку сповістити таких осіб, бажано в письмовому вигляді. Це дозволить тим, чиї інтереси можуть постраждати в результаті такого витоку, також вчасно розробити механізм захисту і вчасно вжити необхідних заходів.

Можливим способом реагування на промислове шпигунство є також звернення із заявою до правоохоронних органів.

Судова практика щодо переслідування винних у зборі та розголошення інформації, що становить комерційну таємницю, досить слабка в Україні, з огляду на той факт, що часто визначити розмір збитку від витоку інформації досить непросто.

Необхідно відзначити, що кримінальна відповідальність за незаконне збирання та умисне розголошення без згоди власника інформації, що становить комерційну таємницю, настає тільки в тому випадку, якщо такий збір та розголошення завдало істотну шкоду суб’єкту господарської діяльності (ст. ст. 231, 232 Кримінального кодексу України).

Однак кримінальна відповідальність без обов’язкової умови заподіяння шкоди передбачена за несанкціоноване втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж або мереж електрозв’язку і за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп’ютерах, автоматизованих системах, комп’ютерних мережах або на носіях такої інформації.

Також у випадку встановлення факту незаконного збирання інформації, що становить комерційну таємницю, можна звернутися до Антимонопольного комітету України. У цьому випадку в Комітет необхідно буде надати докази того, що збір такої інформації здійснювався незаконними методами. Однак в результаті розгляду справи щодо порушення законодавства про захист від недобросовісної конкуренції Комітет може тільки накласти штраф, а для відшкодування завданих збитків необхідно звертатися до суду.

Нормативними актами, що регламентують розгляд органами Антимонопольного комітету України справ про захист від недобросовісної конкуренції, є Закон України «Про захист від недобросовісної конкуренції», Закон України «Про захист економічної конкуренції», Правила розгляду заяв і справ про порушення законодавства про захист економічної конкуренції.

Сума штрафу, який може бути накладений при встановленні Антимонопольним комітетом факту недобросовісної конкуренції у разі збору незаконними методами інформації, що становить комерційну таємницю, може бути в розмірі до 5% доходу від реалізації продукції (товарів, робіт, послуг) суб’єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф. Якщо ж відомостей про дохід немає – то в розмірі до 170 тис. грн. Сума штрафу зараховується до державного бюджету.

Необхідно відзначити, що судова практика щодо переслідування винних у збиранні та розголошенні інформації, що становить комерційну таємницю, досить слабка в Україні, з огляду на той факт, що часто визначити розмір збитку від витоку інформації досить непросто. Крім того, якщо промислове шпигунство було здійснене співробітником, довести його вину буває практично неможливо.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Практика показує, що судове переслідування за промислове шпигунство в світі також рідко закінчується на користь позивача. Крім того, багато компаній вважають за краще не розголошувати факт промислового шпигунства їх діяльності.

**2. Комерційна таємниця**

Наразі чинний Кодекс законів про працю України не містить положень, які регулюють обов’язок працівників щодо нерозголошення комерційної таємниці підприємства. Одним із шляхів вирішення цієї проблеми і методом захисту комерційної таємниці є прийняття на підприємстві локального нормативного акта який би визначав перелік інформації, що становить комерційну таємницю та відображав порядок її використання, зберігання та поширення, а також відповідальність працівників за її несанкціоноване розповсюдження — Положення про комерційну таємницю.

*Загальні положення*

Поняття комерційної таємниці наведено у ст. 505 Цивільного кодексу України, згідно з якою комерційна таємниця ― це інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв’язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру.

Основою для розроблення Положення про комерційну таємницю є перелік відомостей, що становлять таку таємницю, який може бути:

― окремим локальним нормативним актом;

― оформлений окремим розділом Положення про комерційну таємницю;

― додатком до Положення про комерційну таємницю.

Під час формування зазначеного переліку слід пам’ятати, що не вся інформація може бути комерційною таємницею. Складаючи такий перелік слід керуватись постановою Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. № 611.

Структура документа

Структура та зміст Положення про комерційну таємницю залежить передусім від специфіки роботи підприємства та від видів інформації, яка охороняється.

Положення про комерційну таємницю може складатись з наступних розділів:

1) загальні положення;

2) перелік відомостей, що становлять комерційну таємницю підприємства;

3) доступ до комерційної таємниці та обов’язки працівників;

4) відповідальність за порушення Положення про комерційну таємницю.

*Зразок*

*Положення про комерційну таємницю*

1. Загальні положення

1.1. Положення про комерційну таємницю ТОВ «Інновація» (далі ― Товариство) розроблене на підставі Цивільного кодексу України, Господарського кодексу України, постанови Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. № 611 та є локальним нормативним актом, який встановлює права, обов’язки, відповідальність працівників у сфері забезпечення збереження комерційної таємниці.

1.2. Положення визначає обов’язковий для всіх працівників порядок віднесення інформації до «інформації, що становить комерційну таємницю Товариства», та правила зберігання і доступу до такої інформації, можливості її розкриття та передавання третім особам.

1.3. Дія цього Положення спрямована на запобігання можливому економічному збитку для Товариства і поширюється на будь-яких осіб, яким комерційна таємниця Товариства стала відома через їх посадову чи іншу діяльність.

1.4. Вимоги і правила, викладені в цьому Положенні, обов’язкові для виконання всіма працівниками, посадовими особами Товариства.

1.5. Комерційна таємниця ― відомості науково-технічного, технологічного, фінансово-економічного та іншого характеру, що мають дійсну або потенційну комерційну цінність, що не належать до державних таємниць, розголошення (передача, витік) яких може завдати шкоди інтересам Товариства. Власником комерційної інформації, що створена працівником Товариства в межах трудових відносин є Товариство.

2. Перелік відомостей, що становлять комерційну таємницю підприємства

2.1. До відомостей, що становлять комерційну таємницю Товариства, належать:

2.1.1. Відомості про послуги, які надає Товариство:

― собівартість послуг;

― розмір торговельної націнки;

― обсяги виробництва продукції та реалізації послуг;

― відомості про постачальників, продавців та покупців продукції послуг Товариства, клієнтів Товариства;

― відомості про способи надання і реалізації послуг Товариства;

― відомості про кон’єктуру, маркетингові дослідження.

2.1.2. Відомості про управління Товариством:

― відомості про способи та засоби управління Товариством;

― відомості про внутрішню структуру Товариства.

2.1.3. Відомості про фінансову діяльність Товариства:

― відомості про систему оплати праці;

― відомості, що розкривають показники фінансового плану;

― вартість товарних запасів;

― відомості про баланс Товариства;

― відомості про фінансові операції Товариства;

― відомості про стан банківських рахунків Товариства;

― внутрішні бухгалтерські та фінансові звіти;

― відомості про рівень доходів Товариства.

2.1.4. Відомості про плани Товариства:

― відомості про плани розширення та налагодження комерційних та ділових зв’язків Товариства;

― відомості про план закупівель, продажу та інвестицій;

― стратегічний план розвитку Товариства.

2.1.5. Інші відомості:

― відомості про спеціальність, рівень кваліфікації та місце проживання працівників Товариства;

― інші відомості, пов’язані з виробничою, економічною, фінансовою, управлінською та іншою діяльністю Товариства, які не становлять державної таємниці і розголошення яких може призвести до заподіяння шкоди Товариству, спричинити матеріальні збитки і завдати шкоди його діловій репутації.

2.2. Власником інформації, що становить комерційну таємницю, яка отримана під час трудових відносин працівником Товариства, є Товариство.

2.3. Перелік інформації, що не може становити комерційну таємницю, встановлюється чинним законодавством України.

3. Доступ до комерційної таємниці. Обов’язки працівників

3.1. До комерційної таємниці мають доступ наступні працівники:

― генеральний директор;

― головний бухгалтер;

― начальник управління з охорони та безпеки;

― інші працівники, допущені до комерційної таємниці.

3.2. Працівникам Товариства забороняється:

― виносити інформацію, що складає комерційну таємницю за межі території Товариства на паперових та інших носіях;

― використовувати зазначену інформацію під час письмового листування.

3.3. Працівники Товариства зобов’язані:

― забезпечувати належні умови зберігання в таємниці отриманих законним шляхом документів або інших матеріальних носіїв комерційної таємниці;

― не розголошувати інформацію, що становить комерційну таємницю, без згоди Товариства та не надавати її третім особам без письмового дозволу генерального директора Товариства і не використовувати з особистою метою;

― повідомляти Товариство про відомі випадки розголошення комерційної таємниці, чи загрози розголошення інформації, що становить комерційну таємницю;

― передати Товариству у разі розірвання трудового договору всі наявні в своєму розпорядженні матеріальні носії інформації, що становлять комерційну таємницю, які знаходились у них у зв’язку із виконанням ними своїх посадових обов’язків;

― повідомляти генерального директора Товариства про втрату або недостачу документів, що містять комерційну таємницю Товариства, посвідчень, перепусток, ключів від приміщень, сейфів, особистих печаток, печаток та штампів, а також про причини і умови можливої втрати таких відомостей, незаконне отримання, використання третіми особами інформації, що становить комерційну таємницю;

― не створювати для третіх осіб будь-якими діями чи бездіяльністю можливості отримання комерційної таємниці.

3.4. Працівники Товариства мають право працювати тільки з тими відомостями і документами, що містять комерційну таємницю та конфіденційну інформацію Товариства, до яких вони отримали доступ у силу своїх посадових обов’язків, та зобов’язані знати які конкретно відомості підлягають захисту, а також дотримуватися правил користування ними.

3.5. Відділ кадрів з метою захисту комерційної таємниці повинен ознайомлювати працівників, яким у зв’язку з їх посадовими обов’язками необхідний доступ до інформації, що становить комерційну таємницю, з Положенням про комерційну таємницю.

4. Відповідальність за порушення Положення про комерційну таємницю

4.1. Під розголошенням комерційної таємниці розуміється:

― розголошення інформації, володіння якою входить до кола посадових обов’язків працівника, іншим працівникам, у яких немає до них доступу, а також третім особам, які не є працівниками Товариства;

― розголошення інформації, яка була отримана випадковим чином, працівникам, які не мають доступу до неї, а також третім особам, які не є працівниками Товариства;

― отримання інформації, що становить комерційну таємницю, з використанням спеціальних засобів або шляхом протиправних дій.

4.2. Відповідальність за розголошення комерційної інформації несе кожний працівник Товариства, який має доступ до неї та допустив її розголошення.

4.3. Працівник, який у зв’язку з виконанням посадових обов’язків отримав доступ до інформації, що становить комерційну таємницю, у випадку умисного чи необережного розголошення цієї інформації за відсутності у діях такого працівника складу злочину несе дисциплінарну відповідальність, а у випадках встановлених законодавством цивільно-правову, адміністративну, та кримінальну відповідальність відповідно до законодавства.

4.4. Працівники Товариства несуть відповідальність за допуск до приміщень третіх осіб, проведення ними оглядів, фото- та відео- зйомок об’єктів, що знаходяться на території Товариства, за допуск цих осіб до персональних комп’ютерів.

4.5. Накладення дисциплінарного стягнення і притягнення до матеріальної відповідальності працівників за розголошення комерційної таємниці здійснюється директором Товариства відповідно до Кодексу законів про працю України.

4.6. Притягнення до адміністративної, цивільно-правової і кримінальної відповідальності за розголошення комерційної таємниці відбувається правоохоронними органами за заявою Товариства відповідно до чинного законодавства.

4.7. По кожному виявленому випадку невиконання, або неналежного виконання працівниками Товариства обов’язків по збереженню комерційної таємниці Товариства, проводиться службове розслідування, результати якого оформлюються протоколом.

 У розділі «Загальні положення» визначається призначення Положення про комерційну таємницю, зазначаються нормативно-правові акти, на підставі яких складено це положення, дається визначення термінів та понять, що використовуються у положенні.

Відповідальною за розробку розділу «Перелік відомостей, що становлять комерційну таємницю підприємства» зазвичай є комісія з питань комерційної таємниці, яка попередньо створюється наказом керівника підприємства, та складає перелік інформації, яку підприємство бажає захистити від несанкціонованого розголошення. На практиці до відомостей, що становлять комерційну таємницю, відносять інформацію, пов’язану з господарською діяльністю підприємства, розголошення якої може завдати шкоди його інтересам.

У розділі «Доступ до комерційної таємниці. Обов’язки працівників» закріплюється механізм забезпечення збереження інформації, що є комерційною таємницею. Також в цьому розділі містяться відомості щодо умов доступу працівників до інформації, що визнається комерційною таємницею, порядок видачі документів, відомостей та інформації, яка становить комерційну таємницю, органам державної виконавчої влади, контролюючим і правоохоронним органам, контрагентам, клієнтам підприємства.

У розділі «Відповідальність за порушення Положення про комерційну таємницю» має бути обумовлений зміст відповідальності працівників у випадку розголошення комерційної таємниці. Крім того, в цьому розділі можна окреслити порядок проведення розслідування та оформлення випадків, пов’язаних з розкриттям комерційної таємниці. Відповідальність встановлюється відповідно до діючого законодавства.

Так, у Кримінальному кодексі України містяться дві статті, які визначають кримінальну відповідальність за посягання на комерційну таємницю, це ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» і ст. 232 «Розголошення комерційної або банківської таємниці».

Також за незаконні дії щодо розголошення комерційної таємниці передбачена адміністративна відповідальність, яка встановлена у ст. 1643 Кодексу України про адміністративні правопорушення.

Притягнути працівника до відповідальності за розголошення комерційної таємниці можливо лише у тому випадку, якщо роботодавець після затвердження Положення про комерційну таємницю ознайомить з ним під підпис працівників, допуск яких до комерційної таємниці необхідний для виконання ними своїх трудових обов’язків, та передбачить в Правилах внутрішнього трудового розпорядку обов’язок працівників щодо нерозголошення комерційної таємниці чи підписання окремого документа у вигляді зобов’язання про нерозголошення комерційної таємниці.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Отже, Положення про комерційну таємницю слід розглядати як потенційно вельми потужний юридичний засіб, спрямований на забезпечення ефективного захисту інтересів підприємства. Однак для того, щоб зазначений документ виявився спроможним належною мірою реалізувати такого роду мету, слід додержуватися чіткої логіки дій при його розробці та подальшому вдосконаленні (у разі виникнення такої потреби), а також проводити постійну роботу зі створення належних умов для його виконання.

**ВИСНОВКИ З ТЕМИ**

Як показує світовий досвід – захиститися від промислового шпигунства повністю неможливо. Промислове шпигунство було, є і залишається серйозною загрозою для успішного бізнесу в усьому світі, незважаючи на появу все нових і нових технічних засобів протидії йому та його виявлення. Єдине, що важливо пам’ятати всім компаніям, це те, що профілактика, тобто належний захист інформації, що становить комерційну таємницю, є дуже важливою в сьогоднішніх умовах ведення бізнесу.