**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

# Дніпропетровський державний університет внутрішніх справ

**ЮРИДИЧНИЙ ФАКУЛЬТЕТ**

**КАФЕДРА кримінально-правових дисциплін**

# конспект лекцій НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**ПРАВОВЕ ЗАБЕЗБПЕЧЕННЯ ТА ОРГАНІВЗАЦІЯ ДІЯЛЬНОСТІ НЕДЕРЖАВНИХ СЛУЖБ БЕЗПЕКИ ПІДПРИЄМСТВ**

Освітній ступінь бакалавр

Спеціальність 262 «Правоохоронна діяльність»

Освітня програма \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(назва, дата і № наказу про затвердження ОП)

Форма навчання денна

у 2019/2020 навчальному році

Конспект лекційних занять обговорені та схвалені на засіданні

кафедри кримінально-праових дисциплін

протокол від  \_\_\_травня 2019 року  № \_\_\_\_

**Керівник кафедри**

кандидат юридичних наук, доцент

**Світлана ШАЛГУНОВА**

**\_\_\_\_\_\_\_\_\_\_\_\_**

**Дніпро – 2019**

Лекцію підготував **Риб’янець С.А.** – доцент кафедри кримінально-правових дисциплін юридичного факультету Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук.

**Тема1. Становище, проблеми та організаційно-правові аспекти забезпечення діяльності недержавних служб безпеки**

**ПЛАН**

Вступ

1. Предмет, завдання та зміст курсу.
2. Становище та шляхи удосконалення законодавства що регулює діяльність недержавних служб безпеки
3. Організаційні основи діяльності служб безпеки.

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

**Вступ**.

Важливим кроком у контексті загального реформування економіки є інтеграція в економіко-правове середовище України ринкових фінансово-господарських інструментів. Введення будь-яких нових методів управління економічними процесами вимагають не тільки їх імплементації в організаційно-правову інфраструктуру фінансово-господарських відносин, а й ретельного розроблення конкретних схем їх застосування з тим, щоб отримати найбільш ефективний результат. Це питання є принциповим тому, що від перших успіхів нововведення у вигляді реалізації конкретних проектів залежить майбутнє його використання у підприємницькій діяльності загалом.

З перших років переходу України до ринкового типу економіки дуже гостро постає питання забезпечення безпеки здійснення економічної діяльності, зокрема на мікрорівні — рівні суб'єктів господарювання.

1. **Предмет, завдання та зміст курсу**

В Україні особливого значення набуває проблема створення сприятливого клімату для підприємництва, його цивілізований розвиток, активізація інвестиційної діяльності, захист прав і інтересів від протиправних зазіхань. Це питання є очевидним і постійним, оскільки суттєві соціально-економічні зміни, що відбуваються в українському суспільстві останніми роками істотно впливають на відповідні правовідносини.

З метою розвитку ринкових відносин в Україні проголошено свободу підприємницької діяльності. Стаття 2 Закону України "Про підприємництво" зазначає, що суб'єктами підприємницької діяльності (підприємцями) можуть бути: громадяни України, інших держав, особи без громадянства, не обмежені законом у правоздатності або дієздатності; юридичні особи всіх форм власності, встановлених Законом України "Про власність; об'єднання юридичних осіб, що здійснюють діяльність в Україні на умовах угоди про розподіл продукції. Але яка саме діяльність є підприємницькою? Згаданий Закон дає визначення підприємництва: "Підприємництво - це безпосередня самостійна, систематична, на власний ризик діяльність по виробництву продукції, виконанню робіт, наданню послуг з метою отримання прибутку, яка здійснюється фізичними та юридичними особами, зареєстрованими як суб'єкти підприємницької діяльності у порядку, встановленому Законодавством".

Головною діючою особою ринку в недержавному секторі економіки і стрижнем будь-якої економічної системи, побудованої не на державно-монополістичних, а на конкурентних засадах є підприємець. Підприємець виступає гарантом стабільності цивільного суспільства, гарантом економічної безпеки держави. Але необхідно зазначити, що повсякденна практика недержавних об'єктів економіки свідчить про їх підвищену порівняно з державними структурами уразливість від протиправних та інших посягань з боку різного роду кримінальних структур, а також окремих осіб. Власність тепер зобов'язує підприємців займатись діяльністю, яка раніше була виключно прерогативою спеціальних державних органів. Забезпечення безпеки приватної діяльності стає важливою необхідністю, є підгрунтям функціонування недержавних об'єктів.

Отже, охорона підприємництва і забезпечення безпеки підприємницької діяльності є стрижневою проблемою, що обіймає комплекс організаційно-правових, техніко-технологічних, адміністративних, виховних, фінансових і спеціальних заходів, спрямованих на виявлення, попередження і припинення загроз і зазіхань на стабільність функціонування і розвитку підприємства. Цей процес містить у собі охорону приватної власності підприємства і фізичний захист його персоналу.

При цьому до власності відносять, по-перше, *основне матеріальне майно*: приміщення, земельна ділянка, парк техніки, сировина й інвентар, а також допоміжне устаткування, призначене для збереження, переробки і перевезення вантажів. По-друге, сюди ж варто віднести *інтелектуальну власність*, що складає інформацію, яка є активом компанії про власність власника, а також знання і досвід співробітників підприємства, їхні професійні секрети і винаходи. Підприємці, які прагнуть мати власну службу безпеки, не повинні розглядати витрати на її створення, як необгрунтовано високі, оскільки життя цінується набагато вище.

1. **Становище та шляхи удосконалення законодавства що регулює діяльність недержавних служб безпеки**

Однією із основним проблем у розвитку законодавства про недержавні служби безпеки з забезпечення економічної безпеки суб’єктів господарювання в Україні є нерозвинута правова база, що гальмує розвиток цієї сфери діяльності. Говорячи про формування правової основи діяльності недержавної системи безпеки підприємництва, слід звернути увагу на важливість відповідного положення, закріпленого статті 3 Закону України »Про підприємництво», ( в ньому зокрема сказано про те, що підприємці мають право без обмежень приймати рішення та здійснити будь-яку діяльність, що не суперечить діючому законодавству, таке формулювання ,якщо його прийняти за основу організації безпеки підприємництва, дає простір для прояву ініціативи, винахідливості й принципів у стислі строки. Може задовольнити попит на всі види без пекових послуг на відповідному ринку Україні. Проте широкість формулювання у сфері без пекових послуг приховує в собі певні складнощі, що диктуються специфікою діяльності.

Дослідження теоретико-правових основ діяльності держави у сфері національної безпеки є вкрай важливим напрямом роботи з погляду становлення і дальшого розвитку системи забезпечення національної безпеки, а також державних і недержавних суб’єктів сектору безпеки України.

Для подолання сучасних викликів і загроз у світі діють відповідно до чинних політичних і правових актів такі основні системи безпеки:

– система міжнародної безпеки, визначена Статутом ООН;

– системи регіональної (субрегіональної) безпеки (НАТО, ОБСЄ, ОДКБ та ін.), існування яких передбачено Статутом ООН та міждержавними двосторонніми й багатосторонніми актами;

– системи національної безпеки, що діють на основі норм законодавства кожної держави та норм міжнародного права.

Водночас можна виокремити низку тенденцій, що ставлять під сумнів ефективність традиційних підходів до безпеки, а саме:

– більшість сучасних конфліктів є внутрішніми, а не міждержавними;

– окремі держави не можуть виконувати основні свої функції щодо соціального захисту, забезпечення стабільності й економічного зростання;

– уряди країн, де відсутні бідність та політична нестабільність, можуть зіткнутися із втратою контролю у багатьох сферах життєдіяльності внаслідок процесів глобалізації та інформаційної революції, що тривають. За цих умов все більше фахівців пропонують розвивати загальносвітові підходи до проблем безпеки, оскільки дослідження у цій сфері уже відійшли від своєї традиційної орієнтації на вивчення зовнішньополітичних проблем та Статут ООН, акти міжнародного і національного права, угоди, договори тощо.

Нині предмет дослідження істотно розширився й поглибився. Враховуючи, що проблеми загроз та безпеки найбільш гостро постають стосовно людини, суспільства і держави, є всі підстави стверджувати, що найбільш тісно загальна теорія безпеки «співпрацює» саме із соціальними і правовими науками, які потребують подальшого розвитку . Зі здобуттям Україною незалежності основну увагу науковці приділяли розробці *теоретичних основ національної безпеки*.

Цій проблематиці присвятили свої праці низка українських вчених. При цьому досліджувались переважно теоретичні засади національної безпеки та відповідний понятійно- категоріальний апарат. Водночас проводилась активна законотворча робота в галузі безпеки. Першим нормативним документом, який на системному рівні врегульовував питання забезпечення національної безпеки стала *Концепція національної безпеки України, прийнята Верховною Радою України у 1997 році*. У 1992 – 2006 роках прийнято низку законів України, зокрема, *«Про Службу безпеки України» (1992), «Про оперативно-розшукову діяльність» (1992), «Про організаційно-правові засади боротьби з організованою злочинністю» (1993), «Про боротьбу з корупцією» (1995), «Про розвідувальні органи України» (2001), «Про контррозвідувальну діяльність» (2002), «Про боротьбу з тероризмом» (2003), «Про Державну прикордонну службу України» (2003), «Про Службу зовнішньої розвідки України» (2005), «Про Державну службу спеціального звязку і захисту інформації України» (2006)* та ін., які створили правові засади діяльності державних суб'єктів сектору безпеки України. Ключовими у визначенні стратегічних і правових засад у цій сфері було прийняття 2003 року Закону *«Про основи національної безпеки України»*, а також *Стратегії національної безпеки України*, схваленої РНБО України й затвердженою в лютому 2007 року Указом Президента України. Звернімо увагу, що Законом «Про основи національної безпеки України» визначено понятійний апарат у цій сфері та об'єкти національної безпеки, зокрема:

* людина і громадянин
  + їхні конституційні права і свободи; суспільство
  + його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне й навколишнє природне середовище і природні ресурси;
* держава
* її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Крім цього, визначено основні ***сфери забезпечення національної безпеки:***

* зовнішньополітичну;
* сферу державної безпеки;
* воєнну та сферу безпеки державного кордону України;
* внутрішньополітичну;
* економічну;
* науково-технологічну;
* екологічну;
* соціальну та гуманітарну сфери;
* інформаційну.

Цим же законом сформульовано основні загрози національним інтересам у різних сферах, визначено основні напрями державної політики у галузі національної безпеки тощо. Одним із ключових з погляду безпеки є також правове закріплення пріоритетів національних інтересів України.

У контексті економічної безпеки до цих пріоритетів віднесено:

– гарантування конституційних прав і свобод людини і громадянина;

– створення конкурентоспроможної, соціально орієнтованої ринкової економіки, забезпечення постійного зростання рівня життя населення;

– збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку;

– забезпечення екологічно і техногенно безпечних умов життєдіяльності громадян і суспільства, збереження навколишнього природного середовища та раціональне використання природних ресурсів;

– інтеграція України в європейський економічний простір, розвиток рівноправних взаємовигідних відносин з іншими державами світу.

Політика національної безпеки, яка здійснювалася Україною з моменту здобуття незалежності, ставила за мету утворення на загальновизнаних принципах і нормах міжнародного права дієвої системи захисту національних інтересів від зовнішніх і внутрішніх загроз. Це потребує розбудови ефективної системи забезпечення національної безпеки та суб’єктів сектору безпеки України, які почали формуватися наприкінці XX століття.

Юридичного визначення сектору безпеки нині не існує. Водночас у більшості європейських країн вважається, що сектор безпеки у широкому розумінні містить:

1) державні сили безпеки – збройні сили, поліція, прикордонні структури, воєнізовані формування, служби внутрішньої безпеки, розвідувальні та митні органи;

2) органи управління і контролю за структурами сектору безпеки – адміністрація президента чи прем’єр-міністра, консультативні ради з питань безпеки, законодавчі органи та профільні парламентські комітети тощо;

3) органи правосуддя та органи досудового слідства – судова влада, міністерство юстиції, органи прокуратури, служба виконання покарань тощо;

4) приватні організації сектору безпеки – охоронні підприємства, недержавні служби безпеки, приватні оборонно-промислові компанії та ін;

5) цивільні організації, які досліджують чи надають консультації з питань безпеки – різного роду громадські організації, аналітичні групи, науково-дослідні інститути, центри, засоби масової інформації тощо.

Правова регламентація законодавства здійснюється з урахуванням інтересів національної безпеки України. В ній визначається діяльність приватних структур і громадських організацій в системі організації національної безпеки як пріоритетних значущих задач. Як формулювалося ще у Постанові Верховної Ради «Про концепцію(основи державної політики) національної безпеки України від 16.01.97 № 3/97-ВР за змінами, внесеними згідно з законами від 21.12.200 № 2171-(2171-14) та від 19.06.2003 № (364-15), визначається що система організації національної безпеки – це організована державою система державних органів, громадських організацій, посадових осіб, окремих громадян, об’єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність в рамках законодавства України. Але варто зазначити, що у переліку структур, які надають без пекові послуги, в даному документі вказуються приватно охороно-технічні, охороні підприємства, інформаційні бюро, навчальні центри, державні служби безпеки, детективні підприємства, сторожова охорона на підприємствах й власні служби безпеки підприємств, в той же час упущена роль громадських організацій сучасному без пековому процесі.

Варто зазначити, що у переліку структур, які надають без пекові послуги, в даному документі вказуються приватно охороно-технічні, охороні підприємства, інформаційні бюро, навчальні центри, державні служби безпеки, детективні підприємства, сторожова охорона на підприємствах й власні служби безпеки підприємств, в той же час упущена роль громадських організацій сучасному без пековому процесі.

Насамперед треба відзначити, що в Україні відсутній окремий закон, який би регулював відносини між суб'єктами права щодо захисту бізнесу чи корпоративних прав, або від зазіхань, як з боку злочинних угруповань, так і з боку корумпованих владних структур. Тож норми права, які регулюють вказані відносини, містяться в окремих законах України та в підзаконних нормативних актах. Найчастіше в цих нормах права особа (як суб'єкт права) виступає не як бізнесмен (тобто особа, що займається підприємницькою діяльністю), а як фізична особа (тобто незалежно від роду занять). Отже, суспільні відносини, пов'язані із забезпеченням безпеки бізнесу, регулюють такі нормативні акти:

1. Конституція України.

2. Кримінальний та Кримінально-процесуальний кодекси України (тобто кодифіковані збірники нормативних актів, що передбачають кримінальну відповідальність за порушення чинного законодавства (у тому числі у сфері безпеки бізнесу), та нормативних актів, що визначають сам процес притягнення винних до кримінальної відповідальності).

3. Кодекс адміністративних правопорушень (тобто кодифікований збірник нормативних актів, що передбачають адміністративну відповідальність за порушення чинного законодавства).

Можна, звісно, заперечити, що який же це захист безпеки підприємницької діяльності, якщо навпаки, кодекси передбачають відповідальність (кримінальну чи адміністративну) за порушення, які вчиняють комерсанти чи фізичні особи при здійсненні комерційної діяльності. Наведемо приклад: є дві комерційні структури, одна ретельно дотримується законів, сплачує податки, при завезенні товару з-за кордону повністю сплачує митні збори, ліцензує свою діяльність — з цих виплат, звісно, складається кінцева ціна товару чи послуг, які фірма реалізує. Інша комерційна структура працює наполовину "в тіні" — не платить податків, завозить контрабандний товар, не ліцензує свою діяльність. Звісно, ціна товару чи послуг у цих двох структурах буде зовсім непорівнянною, внаслідок чого законослухняна комерційна структура збанкрутує, бо не витримає конкуренції з іншою комерційною структурою. Закони ж, встановлюючи покарання за протизаконну діяльність, не дають змоги комерсантам діяти незаконними методами, тим самим підтримуючи здорову конкуренцію та захищаючи права законослухняних конкурентів. Такі приклади можна навести майже по кожній нормі права.

4. Господарський та Цивільний, Господарсько-процесуальний та Цивільно-процесуальний кодекси України.

5. Закони України:

• "Про банки і банківську діяльність";

• "Про цінні папери і фондову біржу";

• "Про акціонерні товариства ";

• "Про інформацію";

• "Про захист від недобросовісної конкуренції";

• "Про захист інформації в автоматизованих системах";

• "Про державну контрольно-ревізійну службу в Україні";

• "Про відновлення платоспроможності боржника або визнання його банкрутом";

• " Про інвестиційну діяльність";

• "Про державну податкову службу в Україні";

• "Про підприємства в Україні";

• "Про аудиторську діяльність";

• "Про оперативно-розшукову діяльність";

• "Про організаційно-правові основи боротьби з організованою злочинністю".

Перелік законів може бути суттєво доповнений, бо майже в кожному з них є норми, які, регулюючи діяльність суб'єктів права, обмежуючи його права у вчиненні протизаконних дій, тим самим забезпечують безпеку підприємницької діяльності законослухняного суб'єкта права.

6. Декрети Кабінету Міністрів, постанови Кабінету Міністрів, положення Національного банку України, інші підзаконні нормативні акти виконавчої влади та відомчі накази та інструкції.

Основні проблеми безпеки підприємницької діяльності в Україні:

• по-перше, ринкова економіка, побудована на конкуренції, є дуже динамічною системою, а значить і дуже небезпечною;.

• по-друге, український ринок перебуває на стадії становлення і тому його механізми ще не відпрацьовані;

• по-третє, в країні відсутні стійкі норми права захисту інтересів підприємців.

Спеціалісти з безпеки вважають, що одним із шляхів створення для недержавних підприємств передумов для економічного виживання за умов ринкових відносин є виявлення та нейтралізація загроз економічній стабільності підприємства, що і є суттю діяльності щодо забезпечення безпеки підприємства.

Безпека суб'єкта залежить від різних факторів. Шкоду інтересам підприємця може бути завдано у результаті несприятливої економічної політики держави, протиправних дій конкурентів, кризових явищ в економіці, непередбачених змін кон'юнктури ринку, стихійного лиха, надзвичайних подій, управлінської некомпетентності, соціальної напруги тощо.

Отже, фактори, що впливають на рівень безпеки підприємств можуть бути внутрішніми і зовнішніми, економічними та неекономічними, об'єктивними і суб'єктивними.

Виходячи з того, що головним принципом ринкової економіки взаємодія господарчого об'єкта і ринку, який є сукупністю господарчих об'єктів і разом з тим самостійною цілісністю (не зведену до суми складових її частин), господарчий суб'єкт може існувати тільки з умови безперебійної взаємодії з ринковим середовищем. Для цього необхідне нормальне функціонування як самого підприємства, та і ринку в цілому.

Безпека не може бути знеособлена — цілком природно, що небезпека (поняття "загроза") може виходити від когось або чогось (поняття "потенційний супротивник") і спрямована на когось або щось (поняття "об'єкт"). Тепер можна визначити певну формулу безпеки: безпека — стан стійкої життєдіяльності об'єкта стосовно впливу загроз потенційного супротивника.

1. **Організаційні основи діяльності служб безпеки**

З позиції безпекознавчої парадигми недержавна система безпеки може розглядатися у двоякому плані. З одного боку, вона є об'єктом забезпечення безпеки з боку держави, а з іншого - суб'єктом забезпечення власної безпеки, який самостійно визначає мету, принципи та методи забезпечення безпеки згідно з чинним законодавством України. Централізація і монополізація безпеки призводить до послаблення, а у деяких випадках і анемії недержавної системи безпеки, яка має розглядатися не як конкурентна, а як резервна система безпеки. Більше того, рівень демократизації суспільства є прямо пропорційним розвиткові недержавної системи безпеки .

Розглядаючи недержавну систему необхідно зазначити, що її побудова повинна здійснюватись на основі дотримання таких принципів, як:

* законність;
* дотримання прав і свобод громадян;
* централізоване керування;
* координація і взаємодія з правоохоронними органами;
* самостійність;
* відповідальність за забезпечення безпеки;
* відповідність зовнішнім і внутрішнім загрозам безпеки;
* передова матеріально-технічна оснащеність;
* прогресуюче стимулювання суб'єктів системи;
* компетентність;
* конфіденційність;
* корпоративна етика;
* комплексне використання сил і засобів.

Завданнями ж недержавної системи безпеки є охорона і захист законних прав і інтересів підприємницької структури та його співробітників; збір, аналіз, оцінка і прогнозування даних, що характеризують стан обстановки; вивчення партнерів, клієнтів і конкурентів; своєчасне виявлення можливих прагнень до підприємницької структури і його співробітників з боку джерел зовнішніх загроз безпеки; недопущення проникнення до підприємницької структури структур економічної розвідки, організованої злочинності й окремих осіб із протиправними намірами; протидія технічному проникненню в злочинних цілях; виявлення, попередження і припинення можливої протиправної й іншої негативної діяльності співробітників господарюючого суб'єкта на шкоду його безпеки; захист співробітників підприємницької структури від насильницьких зазіхань; схоронність матеріальних цінностей і відомостей, що складають комерційну, банківську, іншу таємницю, що охороняється законом; добування необхідної інформації для найбільш оптимального вироблення управлінських рішень з питань стратегії і тактики економічної діяльності; фізична і технічна охорона будинків, споруджень, території і транспортних засобів; формування в засобах масової інформації, у партнерів і клієнтури сприятливої думки про підприємницьку структуру, що сприяє реалізації планів економічної діяльності; відшкодування матеріального і морального збитку, нанесеного в результаті неправомірних дій організацій і окремих осіб; контроль за ефективністю функціонування системи безпеки.

Надійність і ефективність функціонування системи оцінюється за критеріями: відсутності, або своєчасного виявлення спроб несанкціонованого проникнення до підприємницької структури у злочинних цілях; недопущення фактів витоку, розголошення відомостей, що складають комерційну й іншу таємницю, що охороняється законом, втрати важливих документів, виробів; попередження протиправних і негативних проявів з боку персоналу господарюючого суб'єкта; схоронності матеріальних цінностей, фінансів; припинення насильницьких зазіхань на життя і здоров'я співробітників; попередження надзвичайних подій. Головним же критерієм оцінки ефективності і якості системи є стабільність фінансового й економічного розвитку підприємницької структури відповідно до намічених планів і задач у різних умовах обстановки.

Системний підхід до безпеки підприємництва має бути:

* безупинним - вимога, яка не дає можливості зловмисникам обійти захист для досягнення своїх протиправних цілей;
* централізованим - у межах визначеної підприємницької структури повинна гарантуватися організаційно-функціональна самостійність процесу забезпечення безпеки;
* плановим - розробка планів дій щодо забезпечення захищеності організації всіма компонентами його структури;
* універсальним - незалежність заходів безпеки від місця їхнього можливого впливу;
* активним - захисні заходи перетворюються в життя з достатнім ступенем наполегливості;
* надійним - надійність методів, засобів і форм захисту з одночасним дублюванням засобів і заходів безпеки;
* комплексним - застосовування усіх видів і форм захисту в повному обсязі.

Отже, забезпечення безпеки недержавною системою, спрямоване на захист законних прав та інтересів підприємців і сприяє загальному розвитку підприємництва в Україні. Недержавна система забезпечення безпеки підприємництва та особи виступає об'єктивним союзником державної системи і це визначає можливість і необхідність взаємодії державних служб і органів безпеки з представниками недержавної системи безпеки.

Світовий досвід показує, що така взаємодія розширює можливості держави в боротьбі з економічними злочинами, із загальнокараною злочинністю, із промисловим шпигунством і економічною розвідкою.

**Тема2. Принци формування недержавних служб безпеки підприємств (як складової національної безпеки)**

План.

Вступ.

1.Основні напрямки діяльності служб безпеки підприємств

2. Взаємодія НСБП з державними службами безпеки

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

**Вступ**

Одним із головних завдань соціальної та правової держави є забезпечення конституційних прав людини на захист своїх законних прав та інтересів. Виконання цього завдання відбувається шляхом створення системи правоохоронних органів. Проте діяльність лише державних правоохоронних органів не завжди здатна повною мірою забезпечити конституційне право людини на захист своїх законних прав та інтересів.

Отже, постає необхідність створення альтернативного недержавного правоохоронного механізму.

Сучасний світовий досвід свідчить про те, що чимало країн світу у забезпеченні правопорядку та безпеки покладаються не лише на державні правоохоронні органи, але й на недержавні суб'єкти правоохоронної діяльності. Частка працівників недержавних правоохоронних структур у ряді країн світу, зайнятих в індустрії забезпечення безпеки, коливається від 50 % до 80 % від загальної кількості осіб, професійно зайнятих боротьбою зі злочинністю.

В Україні дотепер такий вид діяльності нормативно не закріплено, у законодавстві відсутнє і саме поняття "недержавна правоохоронна діяльність". Порядок здійснення недержавної правоохоронної діяльності в Україні регулюється як нормами публічного, так і нормами приватного права. Правовим підґрунтям для здійснення додержавної правоохоронної діяльності в Україні є положення ст. 3 Конституції України, яка встановила, що людина, її життя та здоров'я честь і гідність, недоторканність і безпека визнаються найвищою соціальною цінністю, положення ч. 4 ст. 55 Конституції, яка закріпило право кожного захищати свої права і свободи від порушень і протиправних посягань будь-якими не забороненими законом засобами та положення ч. 1 ст. 59 Конституції України, котра встановила, що кожен має право на правову допомогу.

У публічно-правовій сфері спеціальною правовою основою для здійснення недержавної правоохоронної діяльності є положення ст. 38 КК України.

**1.Основні напрямки діяльності служб безпеки підприємств**

Нещастям вітчизняних підприємців є те, що, заробивши великі гроші, вони не хочуть усвідомлювати, що багатство неминуче переводить їх у "групу ризику". Як показує сумний досвід, наші підприємці починають здійснювати суттєві кроки із забезпечення власної безпеки лише після того, як у них починаються неприємності.

Побудова ринкової економіки в Україні поступово зумовлює створення системи забезпечення безпеки підприємницької діяльності відповідно до світової практики. Важливим чинником цього процесу є утворення функціонування державних і недержавних структур як єдиного цілого. *Складовими єдиної системи забезпечення безпеки особи та підприємництва є*:

1. державна система, що представлена правоохоронними органами та спецслужбами (наприклад, Державна служба охорони при Міністерстві внутрішніх справ, яка діє на засадах самофінансування за рахунок коштів, одержаних за організацію та здійснення за договорами заходів особистої і майнової безпеки громадян і юридичних осіб);
2. недержавна система, яка представлена приватними охоронними, охоронно-технічними підприємствами, комерційними службами безпеки, підприємства різної форми власності, інформаційними бюро, службами безпеки банків, навчальними центрами, профільними фондами, науково-дослідними структурами, профільними факультетами вищих навчальних закладів (прикладом є факультет права і безпеки підприємництва Європейського університету м. Києва).

Слід зауважити, що велику частину недержавної системи складають професіонали, колишні співробітники служби безпеки, органів внутрішніх справ, збройних сил і підрозділів спеціального призначення.

Для порівняння, в західних країнах в підприємницькому секторі головну роботу по захисту бізнесу здійснюють недержавні служби безпеки, численність яких, наприклад в США, вдвічі перевищує штат поліції. А це, в свою чергу, знижує витрати держави на утримання поліції .

Не заперечуючи необхідності і важливості функціонування державної системи безпеки, все ж таки слід наголосити на необхідність і безальтернативність формування недержавної системи безпеки. Вивчення світового досвіду дає можливість стверджувати про позитивну практику функціонування даної системи.

З позиції безпекознавчої парадигми недержавна система безпеки може розглядатися у двоякому плані. З одного боку, вона є об'єктом забезпечення безпеки з боку держави, а з іншого - суб'єктом забезпечення власної безпеки, який самостійно визначає мету, принципи та методи забезпечення безпеки згідно з чинним законодавством України. Централізація і монополізація безпеки призводить до послаблення, а у деяких випадках і анемії недержавної системи безпеки, яка має розглядатися не як конкурентна, а як резервна система безпеки. Більше того, рівень демократизації суспільства є прямо пропорційним розвиткові недержавної системи безпеки .

Виникнення недержавної правоохоронної діяльності в Україні на початку 90-рр. XX ст. пов'язане з докорінними перетвореннями, які відбулись у політичній, економічній та правовій сферах суспільства. Саме за умов підвищеної криміногенної ситуації у країні, зростання корупції, недосконалості юридичних механізмів захисту прав людини виявилася нездатність державних правоохоронних структур мобільно та повністю власними силами забезпечити безпеку у всіх соціальних сферах життєдіяльності суспільства. Це, з одного боку, обумовило виникнення недержавного сектора правоохоронної діяльності, котра покликана захищати осіб, що займаються професійною діяльністю, пов'язаною з підвищеним ризиком для життя та безпеки (підприємці, журналісти тощо), а також задовольняти потреби суспільства у послугах охоронного характеру. З іншого боку, здійснення недержавної правоохоронної діяльності обумовлюється тим, що вона у певних випадках виступає як підприємницька діяльність, метою якої є одержання прибутків.

Основні ознаки, характерні для державної і недержавної правоохоронної діяльності:

**1.** Недержавна правоохоронна діяльність може здійснюватися лише за допомогою застосування юридичних заходів впливу, визначених у конкретному законі. До них належать заходи запобігання, припинення та адміністративно-процесуального забезпечення.

**2.** Застосовування заходів юридичного впливу, яке повинно суворо відповідати приписам закону або іншого правового акту (наприклад, договору). Тільки закон або інший правовий акт можуть слугувати підставою застосування конкретного заходу юридичного впливу й чітко визначати його зміст.

**3.** Реалізація їх у встановленому законом порядку з дотриманням певних процедур.

**4.** Реалізація цієї діяльності покладається насамперед на спеціально створені підприємства, що пройшли державну реєстрацію й одержали ліцензію на право здійснення певного виду недержавної правоохоронної діяльності. Комплектуються ці підприємства відповідним чином підготовленими фахівцями — здебільшого особами, які володіють знаннями у галузі юриспруденції, криміналістики та інших дисциплін, які пройшли спеціальну підготовку й одержали державну ліцензію. Організація й діяльність таких підприємств детально та всебічно регламентуються у законодавчому порядку, зокрема відомчими підзаконними актами різних міністерств і відомств, що встановлюють окремі процедурні правила під час вирішення найбільш відповідальних питань.

Здійснюється у суворій відповідності із принципами, притаманними правоохоронній діяльності.

Характерними рисами, що відрізняють недержавну правоохоронну діяльність від державної, **є мета здійснення (передусім захист недержавних інтересів), суб'єктний склад (носії недержавної правоохоронної діяльності не є офіційними агентами держави), неможливість застосування до правопорушників у ході її реалізації заході юридичної відповідальності.**

Відмінні риси, що диференціюють недержавну та державну правоохоронну діяльність:

**1.** У ході здійснення недержавної правоохоронної діяльності підлягають охороні та захисту недержавні (приватно-правові) інтереси Захист суспільних, державних інтересів у цій ситуації є переважно похідною метою.

**2.** Недержавні правоохоронні суб'єкти (носії недержавної правоохоронної діяльності) не виступають від імені держави, не є її агентами або повноважними офіційними представниками, а діють винятково за дорученням своїх клієнтів, що їх найняли, від їхнього імені.

**3.** Недержавні правоохоронні суб'єкти у ході здійснення недержавної правоохоронної діяльності не мають права застосовувати до порушників закону заходи юридичної відповідальності, включаючи санкції.

Види недержавної правоохоронної діяльності:

**• комерційна та некомерційна;**

**• охоронно-детективна та правозахисна (адвокатська);**

**• освітня діяльність у галузі недержавної правоохоронної діяльності;**

**• діяльність, що здійснюється на користь індивідуально визначених** осіб (клієнтів) та діяльність, що здійснюється на користь необмеженого кола осіб).

Основні функції недержавної правоохоронної діяльності:

**• правозахисна;**

**• превентивна;**

**• охоронна;**

**• детективна;**

**• функція кримінальної або адміністративної юстиції*.***

*Основні напрямки діяльності НСБП*

Реалізацію концептуальних положень НСБП буде здійснено через:

* розвиток різних форм співробітництва між зацікавленими представниками законодавчих органів, економічних і правоохоронних відомств, ділових кіл, суспільних об'єднань підприємців, приватних детективних (в перспективі) і охоронних служб, наукових установ і засобів масової інформації
* розробку і суспільну експертизу законодавчих ініціатив і проектів нормативних актів з питань безпеки підприємництва і охорони комерційної таємниці, проведення досліджень з проблем забезпечення економічної безпеки України;
* сприяння формуванню механізмів і процедур компетентного прийняття рішень в області охорони прав особистості, забезпечення економічної безпеки, управління інвестиційними ризиками, боротьби з недобросовісною конкуренцією, розвитку системи охорони громадсько-правових відносин;
* сприяння розвитку послуг в області безпеки підприємництва, формування ділової етики учасників цього ринку і упорядкування діяльності недержавних служб безпеки;
* підготовку рекомендацій і участь в організації міжнародного співробітництва в сфері забезпечення безпеки підприємництва, зниження інвестиційних ризиків і захисту зарубіжних ділових партнерів від злочинних посягань на території України;
* підтримку ініціативних досліджень і інноваційних ідей, вивчення і розповсюдження міжнародного досвіду з питань боротьби з економічною злочинністю;
* здійснення охоронних заходів і захисту інформації;
* організацію взаємодії правоохоронних органів і недержавних служб безпеки недержавного сектора економіки;
* інформування суспільства з питань забезпечення безпеки підприємництва, та практики взаємодії державних органів і приватних структур в боротьбі з правопорушеннями в сфері економіки;
* розробку баз даних нормативно-правових документів, що регламентують діяльність суб'єктів НСБП;
* розробку і реалізацію навчальних програм та видавницьких проектів, спрямованих на підвищення безпеки кожної людини і родини.

**2. Взаємодія НСБП з державними службами безпеки**

Взаємодія з державними структурами в сфері забезпечення безпеки підприємництва буде організовано в наступних напрямках:

* фізична охорона різного роду об'єктів і приватних осіб з використанням сучасних технічних та спеціальних засобів;
* інформаційна безпека суб'єктів економічних відносин, в тому числі захист комерційної таємниці;
* інформаційно-аналітичне забезпечення підприємницького ризику, оцінка перспектив розвитку бізнесу, надання інформації щодо надійності ділових партнерів;
* превентивне консультування підприємців з питань безпеки;
* забезпечення безпеки міжнародних і вітчизняних виставок, конгресів, симпозіумів, фестивалів тощо;
* надання підприємницьким структурам гарантій з безпеки та інформування щодо надійності партнерів при здійсненні комерційних операцій;
* планові патрулювання в громадських місцях спільно з підрозділами патрульної служби поліції під час проведення масових культурно-просвітницьких і соціальних заходів;
* забезпечення силами недержавних служб безпеки громадського порядку в місцях проведення масових спортивних і видовищних заходів;
* підготовка та перепідготовка кадрів як в державних, так і недержавних учбових закладах, розробка та запровадження з цією метою відповідних освітніх програм;
* залучення іноземних інвестицій на засадах гарантування надійності українських суб'єктів господарювання та безпеки їх бізнесу;
* розробка та впровадження реєстру суб'єктів НСБП;
* підготовка підприємців для здійснення безпечного бізнесу.

Для забезпечення взаємодії суб'єктів НСБП та органів державної влади утворюються відповідні Координаційні ради. Доцільно утворити такі ради при: Службі безпеки України, Міністерстві внутрішніх справ, Міністерстві економіки та з питань європейської інтеграції, Державній подактовій адміністрації, Міністерстві юстиції, Торгово-промисловій палаті.

Світовий досвід показує, що така взаємодія розширює можливості держави в боротьбі з економічними злочинами, із загальнокараною злочинністю, із промисловим шпигунством і економічною розвідкою.

Налагоджена взаємодія державної і недержавної правоохоронних систем повинна благотворно впливати на підприємницьку діяльність, що вигідна усім: підприємцям, громадянам, суспільству і державі. Продумана і раціонально організована взаємодія недержавної системи з правоохоронними органами є одна з найважливіших складових ефективності захисту підприємства.

Необхідність активної взаємодії органів внутрішніх справ і недержавної системи виникає також через наявність єдиної інформаційної мережі в сфері контролю за кримінальною діяльністю з одного боку й об'єктивно існуючої обмеженості джерел інформації по цьому питанню з іншого. При цьому керівників служб безпеки підприємства в першу чергу можуть цікавити відомості, що зберігаються в міських і обласних адресно-довідкових бюро (прописка, реєстрація, виписка і т.д.), інформаційних центрах управління внутрішніх справ (відомості про судимість в осіб, що перевіряються, про порушення чи припиненню відносно нього кримінальної справи, про відмовлення в порушенні кримінальної справи). У свою чергу представникам оперативних і слідчих органів внутрішніх справ можуть бути дуже корисні відомості про факти крадіжок з об'єктів, що охороняються і несанкціонованих проникнень зловмисників на об'єкт; про підозрілих осіб, які затримані охороною підприємства на території об'єкта; про сумнівних клієнтів чи недобросовісних конкурентів підприємства; про співробітників охорони, звільнених по підозрі у зв'язку зі злочинцями.

Процедурна взаємодія, спільні дії служби безпеки і правоохоронних органів можуть відбуватися як на договірній, так і на недоговірній основі. Якщо можливість спільних дій не передбачається в договорі, то їм, як правило, передує усна домовленість про допомогу і підтримку. Це часто відбувається у випадках, коли органи міліції розташовані поруч з об'єктом чи коли суміжні об'єкти (території, приміщення і т.д.) охороняються міліцією і приватною охороною.

Отже, діяльність по організації взаємодії недержавних служб безпеки підприємств з правоохоронними органами з питань, що представляють взаємний інтерес, повинна бути спрямована на вирішення концепції безпеки підприємництва. Керівникам усіх рангів і рівнів у сфері забезпечення безпеки необхідно чітко усвідомлювати, що участь в організації взаємодії вимагає глибокого аналітичного дослідження. Гарантією якісних результатів на цьому напрямку роботи є чесність і гідність, досвід і кваліфікація осіб, які здійснюють реалізацією процесу оперативної взаємодії.

**Тема 3. Формування недержавної системи безпеки підприємства в Україні.**

План:

Вступ

1. Передумови створення недержавних служб безпеки підприємств в Україні
2. Система корпоративної безпеки УСПП (Український союз промисловців-підприємців) як тимчасовий координаційний центр формування недержавної системи безпеки підприємств.

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

**Вступ**

Діяльність підприємств за умов ринку характеризується передусім певним рівнем економічної свободи суб'єктів господарювання. Однак свобода одного учасника ринкових відносин обмежується правами та економічною свободою інших суб'єктів господарювання, які прагнуть насамперед власної вигоди. Таке поняття, як вигода, є майже ключовим у причинно-детермінаційному комплексі виникнення ризиків, оскільки вигода одного учасника ринкових відносин може стати руйнівною силою виникнення ризику, збитків, втрат і навіть банкрутства для інших учасників. Це положення посилюється ще й тим, що підприємства, які виробляють однорідну продукцію або надають подібні послуги, прагнуть у будь-який спосіб витіснити свого конкурента з ринку або хоча б посісти домінуюче положення.

Отже, учасники економічних відносин незалежно від власного бажання протягом своєї діяльності будуть мати справу з певним рівнем невизначеності і, як наслідок цього, відчувати на собі вплив тих видів ризиків, які притаманні ринковій економіці взагалі та конкретним економічним умовам країни в цілому або тому чи іншому напрямку діяльності зокрема.

Умови невизначеності, які існують у будь-яких видах економічної діяльності, е предметом досліджень і об'єктом постійного спостереження фахівців різних галузей науки — юристів, економістів, соціологів, політологів тощо. Комплексність підходу до вивчення цієї проблеми зумовлюється тим, що суб'єкти господарювання у процесі своєї діяльності залежать від цілої низки умов, залежно від їх причинного складу та місця виникнення, а саме: соціально-політичних, адміністративно-управлінських, законодавчих, виробничих, комерційних, фінансових. Поняття ризику як об'єктивного прояву невизначеності з'явилося у військових, економічних, демографічних, медичних, біологічних, правових та інших дисциплінах. У вищих навчальних закладах багатьох країн дедалі більше уваги приділяється проблемі вивчення методів управління ризиками.

1. **Передумови створення недержавних служб безпеки підприємств в Україні**

Сьогодні у наукових та періодичних фахових джерелах можна знайти багато різних за обсягом та багатогранністю визначень "ризику". Це обумовлюється насамперед багатоаспектністю цього явища, а також практично повною відсутністю його законодавчого врегулювання.

*Ризик* — це ймовірність виникнення збитків або недоодержання прибутків порівняно із варіантом, що прогнозується.

Сутність ризику як феномену характеризує взаємозв'язок таких основних його елементів:

• можливість відхилення від передбачуваної мети, заради якої здійснюється вибір одного з альтернативних рішень;

• імовірність досягнення бажаного результату;

• відсутність упевненості в досягненні поставленої мети;

можливість матеріальних, моральних та інших втрат, пов'язаних із втіленням у життя вибору, зробленого за наявності альтернативи, за умов невизначеності.

У літературі, присвяченій вивченню теорії ризиків, висвітлюються різні засади їх класифікації. Вони дозволяють проаналізувати найзагальніші ознаки класифікації ризиків, що можуть виникати під час економічної діяльності.

Існують загальні зовнішні джерела загрози функціонуванню підприємства, а саме:

• несприятлива для підприємства економічна політика держави. Маніпулювання (з метою регулювання економіки) валютним курсом, ставками митного тарифу, податків і т. ін. можуть вступати у протиріччя виробництву, комерційній і фінансовій політиці держави. Крім вищезгаданого, реальну загрозу для підприємства становлять адміністративні дії влади, насильницьке звуження сфери товарно-грошових відносин, порушення (з боку державних органів) законів, що регламентують підприємницьку діяльність, перевищують встановлену компетенцію у взаємовідносинах із підприємством, необґрунтоване втручання в його виробничу, фінансову і комерційну діяльність, зазіхання на власність підприємства і т. ін.

• при виході на зовнішні ринки підприємство може також зазнати негативного впливу внаслідок несприятливої економічної політики іноземних держав.

• джерелом зовнішньої загрози для комерційної діяльності підприємства є дії деяких господарчих суб'єктів. Насамперед ідеться про недобросовісну конкуренцію, яка, до речі, різними джерелами трактується по-різному.

• руйнації, пов'язані із землетрусом, повінню (затопленням), пожежею, аваріями енергопостачання, радіаційною небезпекою, небезпекою від впливу сильних акустичних і електромагнітних полів.

Загрози приміщенням, устаткуванню, транспорту можуть бути спрямовані або на їх знищення (розплата за щось), або на внесення істотних обмежень у їх нормальне функціонування. У цьому випадку загрози можуть бути реалізовані під виглядом стихійних (аварійних) явищ або під виглядом діянь, що перебувають у полі дії кримінального кодексу, коли передбачене законом покарання незмірно менше завданих збитків.

Загрози персоналу і клієнтам можуть мати як фізичний, так і психологічний характер. Це можуть бути акти насильства, шантажу, замасковані під "гумову" статтю 206 Кримінального кодексу (Хуліганство), а можуть бути і серйозні розборки, про результати яких ми дізнаємося з кримінальної хроніки (з вибухами та вбивствами). Тут також можна простежити дії, спрямовані на примушування виконати визначені умови, або помста за що-небудь (зазвичай вони поєднуються).

Загрози інформації переважно спрямовані на її негласне одержання, знищення (відновлення) і модифікацію. Ці загрози можуть бути реалізовані за допомогою агентів (викрадання, використання сильних світу цього тощо) або за допомогою спеціальних технічних засобів. Як відомо, вартість техніки з приставкою "спеціальна" значно зростає, а заробітна плата потенційних агентів (найманих працівників) такої тенденції не має. Тому вашому потенційному супротивнику у наших умовах вигідніше годувати агента, що працює з вами, ніж купувати техніку з приставкою "спеціальна", залучати осіб, ще її обслуговують, і прокидатися вночі з думкою про те, що вони ще чиїсь агенти. В інших економічних умовах (стабільність, наявність середнього класу (де існує страх найманих працівників втратити роботу назавжди), природно, більш небезпечними є загрози, пов'язані із застосуванням технічних засобів.

Отже, зробимо маленьке відкриття — одержати повний перелік загроз неможливо.

Пояснюючи його, візьмемо до уваги такі узагальнення:

• фізичні загрози присутні як у середовищі, яке вас оточує (стихія, фізичні і хімічні середовища, аномальні явища, етнічне оточення, економіка, політика, право), так і у вигляді таких самих інших, але спеціально створених і реалізованих людиною явищ, актів у правовому полі кримінального кодексу або поза ним. Повні знання про такі загрози та методи їх здійснення повинні охоронятися державою і застосовуватися тільки у випадках, які зачіпають інтереси держави (питання дуже суперечливе, звичайно, але історія свідчить, що саме так і відбувається).

Говорячи про загрози підприємницькій діяльності, потрібно підкреслити, що найбільше поширення в українських реаліях одержали крадіжки, пограбування, розбої, шахрайства, вимагання, хабарництво, зловживання службовим становищем, службова фальсифікація, а також різні форми недобросовісної конкуренції і такі небезпечні форми, як замовлені вбивства і захоплення заручників.

Не будемо також забувати, що все це відбувається на фоні таких притаманних українському ринку особливостей, як:

• несприятлива для підприємця економічна політика держави, що виявляється у маніпулюванні з метою регулювання економіки обліковою ставкою, валютним курсом, ставками митного тарифу і податків;

• руйнування господарських зв'язків;

• штучно знижений курс гривні;

• економічна корупція.

Крім цього, при спробі дати повну картину ситуації, що склалася у сфері української національної економіки, слід враховувати такі особливості нашого ринку:

• розмах промислового і комерційного шпигунства (з боку різних структур, що використовують методи агентурного і технічного проникнення до комерційної таємниці);

• відсутність єдиної стратеги забезпечення безпеки підприємницьких структур;

• відсутність цивілізованих юридичних гарантій для реалізації комерційних інтересів.

Особливу за масштабами в країні і наслідками впливу небезпеку для підприємств становлять рейдерські захоплення і протиправна діяльність кримінальних структур, які створюють реальні загрози не лише окремим підприємствам, але й національній безпеці України.

Процес недружнього поглинання і прямих кримінальних захоплень підприємств в Україні почав набирати масового характеру 2004 року. Цей процес став наслідком неправомірного використання об’єктивних процесів, пов’язаних із трансформацією нашого суспільства в напрямі до формування ринкової економіки.

*По-перше*, в 2004 році відбувся остаточний перехід спочатку від домінування в економіці промислових активів державної форми власності до рівноправних із приватною, а пізніше уже привів і до переваження останньої.

*По-друге*, первинний розподіл виробничих активів за участю держави, як єдиного суб’єкта такого розподілу, закінчився. Значною мірою він перетворився на номенклатурно-кримінальний розподіл загальнонародної власності. Як зауважує з цього приводу експерт, *«поточна хвиля рейдерства, яка розпочалася у період відносного безвладдя, особливо на місцях, у недавній час виборчих кампаній, накрила з головою вже багато українських компаній. І здається, вона матиме значне продовження тому, що через політичні ризики (когось вибрали, когось ні, але всі пов’язані з бізнесом) у деяких компаній справи підуть вгору, а в деяких – навпаки»*.

В результаті була накопичена «критична маса» самовільних управлінських рішень, порушень законодавства і майнових злочинів. Сукупність цих явищ стала основою для появи рейдерства в Україні і його наступного розвитку в характерну негативну особливість національної економіки.

*По-третє*, серед нових власників промислових активів розпочалися процеси майнового розшарування. У них з’явилися власні матеріальні ресурси для участі в наступному перерозподілі національного надбання або ж без участі держави, або ж навпаки: при стимулюванні матеріальної зацікавленості номенклатури, використанні інструментарію адміністративного пресингу стосовно об’єктів рейдерських атак.

*По-четверте*, відбулась трансформація певної частини корумпованих чиновників і політиків, працівників силових структур та представників нової хвилі успішних бізнесменів в новий соціальний прошарок суспільства – вітчизняних олігархів та близьких до них за розміром фінансових можливостей осіб, які активно включилися у новий перерозподіл власності і стали замовниками рейдерських атак.

Ситуація, що склалася в нашій країні уже серйозно турбує економічних партнерів за кордоном. Так, скажімо, на засіданні комітету з питань парламентського співробітництва ЄС – Україна при аналізі економічної ситуації основний доповідач доктор Е. Сечура, головний економіст і глава київського офісу американської компанії Sigma Blazer заявив, що корпоративні рейдери постійно загрожують приватній власності компаній, у світлі чого дуже важливо покращити принципи корпоративного управління. ЄБРР в своєму листі зазначає про «необхідність прийняття нового закону про акціонерні товариства», депутат Євразійського парламенту Г. Станішевська заявляє про те, що багато потенційних інвесторів побоюються юридичної невизначеності в Україні і т. ін.

Отже, рейдерство стало самостійним політико-економічним явищем, що несе в собі чималу загрозу для нормального функціонування держави. В останній час щорічний ринок приватизації та поглинань в Україні складає 3 млрд дол., з яких 60–70% є недружніми поглинаннями (приблизно 2 млрд дол.). Такі обсяги матеріальних ресурсів самі по собі є стимулом для схильних до правопорушень членів суспільства зайнятися такою протиправною діяльністю. Успішність рейдерських атак обумовлюється низкою чинників:

* недосконалістю українського законодавства, і особливо в тій його частині, що встановлює відповідальність за рейдерство. Наприклад, за рейдерські атаки протягом 2005–2006 років жодна особа або компанія, що брали участь у підготовці або здійсненні незаконного поглинання, не були притягнуті навіть до адміністративної відповідальності, не говорячи вже про кримінальну;
* фактами корумпованості представників судової влади, контролюючих та правоохоронних органів;
* високою «рентабельністю» рейдерства – рахується сотнями відсотків прибутку, а рівень ефективності рейдерських атак складає 90 %. Це означає, що лише одній із десяти жертв рейдерів вдається захистити себе та відбити рейдерську атаку;
* слабкою мобілізованістю державних органів та громадськості на вирішення цієї проблеми, недостатнім усвідомленням в суспільстві шкоди, що завдається рейдерством, національним інтересам України та її міжнародному іміджу.

Для досягнення своїх цілей поряд з використанням вказаних чинників рейдери застосовують прийоми недобросовісної конкуренції. Вони, як правило, зводяться до трьох основних напрямів впливу:

– до неправомірного використання ділової репутації суб’єкта господарювання;

– до створення перешкод господарській діяльності та досягнення неправомірних переваг у конкуренції;

– до неправомірного збирання, розкриття та використання комерційної таємниці.

За даними експертів, на сьогодні кількість рейдерських атак в Україні нараховує понад 9000 випадків, а число рейдерських груп досягає 30–50. Про масштаб цього явища свідчить той факт, що об'єктами атак з боку рейдерів вже стали великі компанії, а також підприємства, де утримувачем контрольного пакету є держава.

Як реакція на криміналізацію у сфері підприємницької діяльності в 1991 році в Україні з’явилися перші комерційні структури, що актуалізувалися в сфері охорони майна, забезпечення особистої охорони підприємців, супроводу вантажів і т. п. Серед них «Сакура» (Дічек О., Василенко І.), «Січ» (Балабанов І., Попов Ю.), «Партнер» (Лисюк В., Калінін Г.), «ІBS» (Онищенко Г.) та ін. Уже із самого початку своєї діяльності дані фірми відчули недостатній рівень наявної для даного виду діяльності правової бази. Фактично законодавство стосовно організації безпеки підприємницької діяльності було відсутнє. Фірми, що спеціалізувались на наданні безпекових послуг відчули також потребу в підтримці громадських організацій, в об’єднанні на базі спільних інтересів суспільних зусиль, що забезпечували б підвищення ефективності їх діяльності. У зв’язку із цим у 1993 році за ініціативою Союзу юристів України, Фонду юристів України та фірми «Сакура» була створена перша в Україні громадська організація, що взяла на себе питання організації правового захисту українського підприємництва – Міжнародна неурядова асоціація «Безпека приватного бізнесу» під керівництвом О. Дічека.

Підвищення ефективності діяльності недержавних структур безпеки в цей час уже дозволили значно зменшити вплив негативного явища в вітчизняній економіці, що прямо впливало на рівень національної безпеки – скоротити кримінальний відтік фінансів із України.

Нині можна констатувати початок нового етапу еволюції українського суспільства, що характеризується завершенням процесу конвертації влади в капітал. У підсумку, протягом останніх двох років рейдерство та інші правопорушення в економічній сфері, стали, новим самостійним політико- економічним явищем, що являє собою найбільш видиму, відчутну загрозу для діяльності суб’єктів господарювання, а значить і для нормального функціонування держави.

**2. Система корпоративної безпеки УСПП (Український союз промисловців-підприємців) як тимчасовий координаційний центр формування недержавної системи безпеки підприємств.**

Український союз промисловців і підприємців – найбільше в країні об’єднанння організацій ділових кіл та суб’єктів економічної діяльності усіх форм і видів – від великих вертикально інтегрованих корпорацій до малого й середнього бізнесу. Союз веде історію з 15 лютого 1992 року.

Своєю місією УСПП вважає поширення серед ділової спільноти, громадянського суспільства, органів влади ідеї економічного патріотизму, виборюювання сприятливого підприємницького клімату, відстоювання необхідності багатогранної та ефективної підтримки національного товаровиробника.

В складі УСПП – 28 регіональних відділень, 73 філії та 22 представництва, 34 комісії з різних питань. Серед партнерів Союзу – більше 100 громадських організації, у тому числі Союз хіміків; асоціації міжнародних автомобільних перевізників, «Меблідеревпром», «Укроліяпром», «Укрлегпром», «Виноградарі та винороби України»; Ліга нафтопромисловців; Українська аграрна конфедерація; організація «Міжнародна антитерористична єдність» тощо.

Під егідою Союзу працює Антикризова рада громадських організацій у складі більше 90 всеукраїнських структур, які домовились в екстреному порядку напрацьовувати пропозиції з порятунку економіки, доносити їх зміст до уряду, парламенту та забезпечувати контроль за їх виконанням.

УСПП захищає бізнесменів від бюрократичного свавілля, невмотивованих претензій з боку фіскальних та контролюючих органів, порушення прав та інтересів у стосунках з органами влади, недобросовісними партнерами. Підприємцям надається юридична підтримка – проводяться консультації, готуються заяви, позови до судів.

За ініціативи Українського союзу промисловців і підприємців, який об'єднує 38 тисяч представників різних галузей економіки та форм власності, протягом останніх років інтенсивно напрацьовуються необхідні механізми для створення *недержавної системи безпеки підприємництва* і вперше за роки незалежності почали формуватися недержавні суб’єкти сектору безпеки як складова забезпечення національної безпеки України.

Головним внутрішнім механізмом недержавної системи безпеки підприємництва є укладення соціально-партнерських угод між державними інституціями і суспільством, відповідними громадськими організаціями і підприємцями, об’єднання зусиль державних і недержавних суб’єктів сектору безпеки України. У 2005 році із загостренням об’єктивної потреби розвитку громадянської складової в структурі безпеки приватного підприємництва в Українському союзі промисловців і підприємців була прийнята *Програма з формування політики*, що сприяла б розвитку організаційних засад у цій сфері. В рамках даної Програми були створені Комісія по економічній безпеці і захисту інвестицій, а також відповідне Бюро федерації роботодавців України. Про потребу в організаційному оформлені індустрії безпеки свідчив також і аналіз матеріалів, узагальнення практичного досвіду, що було пов’язано зі створенням Громадянського проекту «Формування недержавної системи безпеки» за ініціативою УСПП, МАЕ та інших креативних у нашій державі громадських організацій.

У жовтні 2006 року за участі та підтримки А.Кінаха, В.Крутова, П.Пригунова, О.Дічека та інших спеціалістів, з урахуванням попереднього практичного досвіду і теоретичних напрацювань, була розроблена *Концепція корпоративної безпеки підприємств – членів УСПП.* Цей факт став помітним явищем у розвитку індустрії безпеки, оскільки дана концепція відобразила інтереси найбільшого в країні громадського об’єднання, що сьогодні виробляє 39 левову частку національного продукту в Україні. Концепція визначила принципи організаційно-правового забезпечення нейтралізації всього комплексу загроз, що призводять сьогодні до дестабілізації в діяльності підприємств – членів УСПП.

Концепція корпоративної безпеки є науково обґрунтованою системою поглядів і розроблена з урахуванням необхідності якнайшвидшої адаптації українських підприємств, що здійснюють зовнішньоекономічну діяльність, до європейських стандартів з безпеки ISO, у зв’язку з інтеграцією у світову економіку і завершенням процесу входження України до СОТ. Визначення мети, цілей та завдань, передбачених концепцією та їх реалізація в рамках діяльності УСПП створили необхідні і достатні умови для розгортання потужної та ефективної системи корпоративної безпеки членів Союзу. Корпоративна безпека членів УСПП стала нині платформою, на якій здійснюється захист інтересів власників, керівництва, працівників і клієнтів підприємств, матеріальних цінностей, інформаційних ресурсів від внутрішніх і зовнішніх ризиків і загроз.

На основі вивчення сучасних викликів і загроз безпеці підприємництву були опрацьовані певні стратегічні параметри та комплекс першочергових заходів розбудови недержавної системи безпеки підприємництва (Системи) за такими напрямами:

1) постійна робота над урахуванням змін в економічній ситуації та інших факторів, що впливають на підприємницьку діяльність, з метою вдосконалення ідеологічних, концептуальних засадах функціонування Системи в Україні;

2) розробка і вдосконалення чинного законодавства відповідно до суспільно-економічних потреб становлення і розвитку Системи;

3) структурування приватних економічних суб'єктів, які надають послуги у сфері безпеки, під егідою УСПП як тимчасового координаційного центру;

4) створення механізмів взаємодії недержавних і державних суб’єктів сектору безпеки на центральному і регіональному рівнях;

5) впровадження в Україні загальновизнаних міжнародних стандартів в галузі безпеки підприємництва;

6) налагодження ефективної взаємодії з найбільш відомими міжнародними компаніями у цій сфері.

Реалізація зазначених стратегічних ініціатив спочатку розпочалася серед підприємств-членів УСПП, які нині виробляють понад 80% валового внутрішнього продукту (ВВП) України. І коли мова йде про такі масштаби та вплив на створення ВВП держави, організація економічної безпеки кожного з членів УСПП – це турбота не тільки про їх процвітання, а фактор утвердження свободи, могутності й достатку всієї України.

Вирішення організаційно-методичних проблем вдосконалення безпеки підприємництва в УСПП було прискорено використанням напрацювань, здійснених громадськими організаціями в рамках *Громадянського проекту по формуванню недержавної системи безпеки підприємництва*. Це унікальний приклад співпраці громадськості й бізнесу. Основною спрямованістю реалізації зазначеної Концепції і Громадянського проекту є:

забезпечення гарантії стабільності розвитку бізнесу кожного суб'єкта господарювання;

забезпечення привабливості підприємництва в Україні для іноземних інвесторів;

зменшення матеріальних витрат і збереження часу підприємця на захист власного бізнесу від протиправних посягань.

У кінцевому рахунку це повинно бути забезпечене побудовою нової архітектури відносин у системі «органи державної влади – підприємці»; створення на загальнодержавному рівні передумов для формування недержавної системи безпеки, як важливої складової національної безпеки України. Для реалізації визначених цілей щодо побудови Системи було сформовано *Раду УСПП з питань корпоративної безпеки,* до роботи якої залучені керівні співробітники органів державної влади і управління, визначні науковці, представники впливових громадських організацій, директори стратегічно важливих підприємств, керівники основних недержавних безпекових структур. Для ретельного аналізу наявних у суб'єктів господарювання проблем, проведення експертних оцінок документів, рішень стосовно забезпечення та реалізації заходів безпеки, було створено *Експертну комісію з питань корпоративної безпеки*, сформовано *Департамент з корпоративної безпеки УСПП*. При регіональних представництвах УСПП введено посади *заступників керівників регіональних представництв з питань безпеки*. Спільно з регіональними відділами УСПП з корпоративної безпеки в регіонах розпочато процес розгортання і налагодження роботи третейських судів (для функціонування цих судів зареєстровано понад 60 суддів в Києві, Полтавській, Запорізькій та інших областях). В їх діяльності вже зафіксовані позитивні результати. Однак, розгортання роботи системи третейських судів поки що не знаходить ефективної підтримки з боку частини представників чинної судової влади, які вбачають в третейських суддях не своїх колег, а конкурентів. Цей суб’єктивний фактор, вважаємо, є тимчасовим і в цілому не зможе зупинити процес організованого громадського впливу на неправові дії стосовно приватного бізнесу.

Крім того, започатковано процес створення мережі страхових компаній, які головною метою своєї діяльності ставлять роботу з корпоративними членами системи безпеки, насамперед, членами УСПП. В цілому, до організаційної структури УСПП увійшло 27 регіональних відділень системи корпоративної безпеки (СКБ). Суттєвим також є залучення до роботи СКБ 371 корпоративного члена УСПП. За ініціативою УСПП в центральних органах виконавчої влади, причетних до забезпечення безпеки підприємництва, визначаються і закріплюються представники в ранзі заступників керівників цих органів, які забезпечуватимуть зв'язки з системою корпоративної безпеки.

Результатом співпраці з Кабінетом міністрів України стало підписання 20 березня 2007 року *Меморандуму про партнерство та співробітництво між Кабінетом Міністрів України та Українським союзом промисловців і підприємців.* Наразі налагоджуються й робочі відносини з Кабінетом Міністрів України, що дозволить:

– продемонструвати суспільству та іноземним партнерам механізми реальної взаємодії виконавчої влади з громадськими організаціями;

– створити новий в українській історії прецедент спільної участі владних структур і структур сфери недержавної безпеки в організації ефективної економічної безпеки в державі;

– організувати сучасну, ефективну систему захисту основних бюджетоутворюючих підприємств;

– системно, а не фрагментарно, підійти до організації безпеки кожного підприємства у різних сферах діяльності (інформаційній, технічній, фізичній тощо);

– залучити до співпраці значну кількість суб'єктів господарювання.

Для налагодження взаємодії між недержавним і державним суб’єктами сектору безпеки за ініціативи УСПП розпочато створення *громадсько- консультативних рад при Кабінеті Міністрів України, МВС України, СБ України, Мінекономіки, Державній податковій службі, Державній митній службі, Адміністрації Державної прикордонної служби та інших органах державної влади*. Зазначені громадські ради розпочали роботу по координації зусиль державних органів, профільних громадських об'єднань, представників промисловості і підприємництва не тільки у сфері захисту суб'єктів господарювання всіх форм власності, але й у боротьбі з екстремізмом, корупцією, організованою злочинністю та іншими зазіханнями на національну безпеку України. Створена й *Координаційна рада МВС України по взаємодії органів внутрішніх справ з охоронними підприємствами, їх об'єднаннями та службами безпеки суб'єктів господарювання.* Згідно з наказом міністра внутрішніх справ від 19.03.2007 № 96 начальникам регіональних органів МВС поставлено завдання щодо створення і забезпечення діяльності відповідних координаційних рад на місцях. В інтересах системи корпоративної безпеки також була створена *Українська національна служба економічної безпеки та захисту інвестицій (УНСЕБ)*, яка теж розгортає свої представництва в регіонах за такими напрямами діяльності:

-консалтинг з питань безпеки бізнесу;

-забезпечення безпеки комерційної діяльності;

-забезпечення безпеки банківської, страхової та інвестиційної діяльності;

-забезпечення технічними засобами безпеки та зв’язку; забезпечення охоронними послугами.

Для розбудови системи корпоративної безпеки УСПП також проведено низку інших заходів. У результаті, нині система корпоративної безпеки має можливість надавати практично повний комплекс послуг у сфері безпеки підприємництва:

фізичну охорону об'єктів та суб'єктів підприємництва,

супровід вантажів,

технічний захист від несанкціонованого доступу до конфіденційної інформації,

проведення бухгалтерського, кадрового, енергетичного та інших видів аудиту,

надання інформаційно-аналітичних і консалтингових послуг у сфері безпеки, юридичної допомоги,

організацію захисту комерційної таємниці,

надання послуг з перепідготовки фахівців в інформаційно-аналітичній сфері,

допомоги в організації служб безпеки,

у боротьбі з рейдерством та інші.

На сьогодні створена в УСПП система корпоративної безпеки підприємництва має чотири рівні функціонування. Цим досягається можливість всебічного захисту діяльності будь-якого підприємства – члена УСПП, створюються умови його сталого розвитку:

*– перший рівень (тактичний)* – коли безпека забезпечується самим підприємством, її службою безпеки на підставі наданих методичних рекомендацій і консультацій СКБ;

*– другий рівень (тактичний регіональний)* – коли безпека забезпечується за допомогою регіонального представництва з залученням регіональних суб'єктів безпеки УСПП – УНСЕБ;

*– третій рівень (тактичний центральний)* – коли безпека забезпечується за допомогою сил апарату, впливу віце-президента УСПП з питань безпеки;

*– четвертий рівень (стратегічний)* – коли безпека забезпечується за допомогою рішень Ради УСПП з питань безпеки із залученням керівних органів державної влади.

Управління цією системою здійснює Рада УСПП з корпоративної безпеки. До суб’єктів забезпечення корпоративної безпеки членів УСПП також відносяться:

– Президент УСПП, Віце-президент з безпеки, Департамент з безпеки;

– Комісія УСПП з питань економічної безпеки суб’єктів господарювання та захисту інвестицій;

– Бюро Федерації роботодавців України з питань координації безпеки бізнесу, енергозбереження та захисту інвестицій;

– Українська національна служба економічної безпеки та захисту інвестицій;

– регіональні представництва УСПП з корпоративної безпеки.

Загалом розглянуте питання можна підсумувати такими основними висновками:

1) система корпоративної безпеки УСПП фактично позиціонує себе як основний системоутворюючий елемент загальнонаціональної системи недержавної безпеки та об’єднує різноманітні сектори ринку послуг у сфері захисту вітчизняного підприємництва. Особливу роль при цьому відіграє Рада УСПП з корпоративної безпеки – інтелектуальний центр для адекватної системної відповіді на сучасні виклики у сфері безпеки підприємницької діяльності. Зі створенням Ради було розпочато процес формування основ цілісного механізму організації недержавної системи безпеки підприємництва, пошук оптимальних форм роботи по вдосконаленню безпеки суспільства і держави в економічній сфері за участі недержавних суб’єктів сектору безпеки;

2) для формування спільних узгоджених позицій з питань організації безпеки підприємницької діяльності, сприяння сталому розвитку підприємств незалежно від їх форми власності, зміцнення правопорядку та громадського порозуміння, забезпечення безпеки громадян, боротьби зі злочинністю, розвитку недержавної системи безпеки, у тому числі шляхом удосконалення чинного законодавства актуальним є питання щодо створення при Кабінеті Міністрів України Експертно-громадської ради з питань безпеки підприємництва;

3) суспільно значимою подією є ініціювання УСПП створення Всеукраїнської громадської організації «Союз недержавних служб безпеки України», який має створити сприятливі умови для розвитку індустрії безпеки, проведення незалежної громадської експертизи законопроектів, що регулюють роботу служб безпеки вітчизняних кампаній; розробки стратегічних напрямів реформування системи безпеки з урахуванням реальних потреб підприємництва; організації аналітичної роботи, наукових і маркетингових досліджень товарів та послуг ринку безпеки тощо;

4) система недержавної безпеки підприємництва, що формується на базі системи корпоративної безпеки УСПП набуває рис повноправної складової національної безпеки України. Надалі актуалізується проблема розвитку системи недержавних суб’єктів сектору безпеки та легітимізації їх діяльності відповідними законами та іншими нормативно-правовими актами України

**Тема 4. Організація діяльності та правове регулювання недержавних служб безпеки в Україні.**

План

Вступ.

1. Правова основа діяльності НСБ
2. Суб’єкти недержавної правоохоронної діяльності та їх місце у забезпеченні безпеки підприємств.
3. Вимоги до працівників недержавних служб безпеки.

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

**Вступ.**

Однією із основних проблем у розвитку недержавної системи безпеки підприємницької діяльності є нерозвинута правова база, що відчутно гальмує розвиток цієї сфери діяльності. Сьогодні надання приватних безпекових послуг здійснюють як фізичні так і юридичні особи. Їх діяльність за своїми ознаками підпадає під визначення підприємницької. Однак, поряд із ними у сфері недержавної системи безпеки підприємництва виникають і успішно діють громадські організації, діяльність яких зосереджена на координаційних, методичних, пропагандистських та інших функціях.

Усі ці суб’єкти діяльності на ринку безпекових послуг, як приватні, так і громадські, в сукупності формують системні риси недержавного сектору безпеки. Ця, створена реальною практикою система, що пов’язана своїм змістом і організаційними принципами із об’єктивними процесами демократизації суспільства, потребує правової підтримки як шляхом уточнення наявних законодавчих актів так і з допомогою нового законотворення.

1. **Правова основа діяльності НСБ.**

Як прийнято у світовій практиці, правова регламентація діяльності недержавних суб’єктів сектору безпеки здійснюється в контексті захисту національних інтересів і національної безпеки України. У Постанові Верховної Ради України «Про Концепцію (основи державної політики) національної безпеки України» від 16.01.97 № 3/97-ВР із змінами, внесеними згідно з законами від 21.12.2000 № 2171-ІІІ (2127-14) та від 19.06.2003 № 964-ІV (964- 15) визначається, що ***система організації національної безпеки*** – це «організована державою система державних органів, громадських організацій, посадових осіб і окремих громадян, об’єднана цілями і задачами по захисту національних інтересів, що здійснюють погоджену діяльність в рамках законодавства України». Але варто зазначити, що у переліку структур, які надають безпекові послуги, в цьому правовому акті вказуються приватні охоронно-технічні, охоронні підприємства, інформаційні бюро, навчальні центри, державні служби безпеки, детективні підприємства, сторожова охорона на підприємствах і власні служби безпеки підприємств, і в той же час упущена роль громадських організацій в сучасному безпековому процесі.

Говорячи про формування правових основ діяльності недержавної системи безпеки підприємництва, слід звернути увагу на важливість відповідного положення, закріпленого в ст. 3 Закону України «Про підприємство». В ньому, зокрема, сказано про те, що *«підприємці мають право без обмежень приймати рішення і здійснювати самостійно будь-яку діяльність, що не суперечить діючому законодавству»*. Таке формулювання, якщо його прийняти за основу організації безпеки підприємництва, дає можливість для прояву ініціативи, винахідливості і, в принципі, у стислі строки може задовольнити попит на всі види безпекових послуг на відповідному ринку в Україні.

Проте широке формулювання саме для сфери безпекових послуг приховує в собі певні складнощі, що диктуються специфікою діяльності. Дія цієї правової норми в ході подальшої законотворчої роботи, була введена в певні організаційні рамки й конкретизована Інструкцією *«Про порядок видачі суб’єктам підприємницької діяльності ліцензій на надання послуг по охороні колективної і приватної власності, а також охороні громадян, монтажу, ремонту і профілактичному обслуговуванню засобів охоронної сигналізації»*, затвердженою наказом МВС України від 28.02.1994 № 112. Даною інструкцією визначається право юридичної особи на подання заяви для отримання ліцензії в управління державної служби охорони УМВС лише в тому випадку, коли в його установчих документах передбачено здійснення послуг у сфері охоронної діяльності колективної і приватної власності та охорони громадян. Інструкція також зобов’язує надавати охоронним підприємствам відповідні послуги лише на основі письмових угод із замовником. Дана відомча інструкція хоча і була певним кроком вперед у формуванні нормативної бази у сфері безпеки підприємництва, однак, не була позбавлена і певних недоліків. За її межами лишилися проблеми громадської участі в процесі формування нового напряму діяльності, що має враховуватись у контексті демократизації суспільства. Інструкція залишила поза увагою загальносуспільні процеси інформатизації в цілому й використання інформаційних технологій як виду розвідувальних і безпекових послуг.

Певним кроком у ліквідації даних проблем став Закон України *«Про господарські товариства»*, введений в дію з 1 жовтня 1991 року. В цьому Законі учасники товариств зобов’язувались не розголошувати комерційну таємницю та конфіденційну інформацію про діяльність даних економічних об’єднань. Посадові особи мають зберігати комерційну таємницю і нести відповідальність за розголошення такої інформації згідно з законом і статутними документами. Поряд із цим, Кабінет Міністрів України прийняв Постанову № 611 *«Про перелік відомостей, що не являють собою комерційної таємниці»*. Згідно з цим документом до комерційної таємниці не відносяться такі документи й відомості:

– документи про заснування економічних структур, що дозволяють займатися підприємницькою, господарською діяльністю або її окремими видами;

– інформація відповідно до встановлених форм державної звітності;

– дані, необхідні, для перевірки нарахування і виплат податків та інших обов’язкових платежів, інформація про чисельність і склад працюючих, про їх заробітну плату, а також про наявність вакантних посад;

– документи про виплату податків і обов’язкових платежів;

– інформація про забруднення навколишнього середовища, що спричиняє шкоду здоров’ю людини, а також про факти інших порушень законодавства України і обсяги нанесених при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємства в підприємницькій діяльності;

– дані, що згідно з чинним законодавством підлягають оприлюдненню.

Вся ця інформація має надаватись органам державної влади, контролюючим і правоохоронним органам України, а також іншим юридичним особам за їх вимогою відповідно до законодавства. У 1996 році було прийнято Закон *«Про захист від недобросовісної конкуренції»*, яким передбачена відповідальність юридичних і фізичних осіб за неправомірне збереження, розголошення та використання інформації, що становить комерційну таємницю. У відповідності із даним законом Антимонопольним комітетом України або ж його філіалами на юридичну особу за такого роду дії може бути накладено штраф, на фізичні особи – адміністративна відповідальність. Кримінальний кодекс України за незаконне збирання даних, що становлять комерційну таємницю, передбачає штрафи, обмеження свободи або ж, зважаючи на тяжкість злочину, позбавлення її. При цьому значною вважається шкода при використанні даних, що є комерційною таємницею, яка в п’ятдесят разів перевищує встановлений законодавством мінімум доходів громадян.

З поширенням в українському суспільстві інформаційно-комп’ютерних технологій та їх використання в пошуковій і охоронній діяльності, виникла суспільна потреба в правовій регламентації цього виду діяльності. У зв’язку з цим у Кримінальному кодексі України було передбачено, що *«незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп’ютерних систем, що призвело до зміни або знищення комп’ютерної інформації чи носіїв такої інформації, а також розповсюдження комп’ютерного вірусу шляхом використання програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп’ютерні мережі і здатних причинити зміну чи знищення комп’ютерної інформації або ж носіїв такої інформації, карається штрафом чи виправними роботами, обмеженням або позбавленням волі. Викрадання, присвоєння, вимагання комп’ютерної інформації або ж заволодіння нею шляхом шахрайства чи зловживання службовим положенням передбачає такі ж міри покарання»*.

Правові заходи, пов’язані із захистом та підвищенням ефективності підприємницької діяльності в умовах розвитку ринкових відносин в Україні, активізації економічної діяльності в період подолання кризових явищ загальнодержавного масштабу знайшли своє відображення також в Указах Президента України, зокрема, в указах від 15.07.2000 № 906 «*Про заходи щодо забезпечення підтримки та подальшого розвитку підприємницької діяльності в Україні*» та від 03.07.2000 № 849 *«Про сприяння підготовці управлінських кадрів для сфери підприємництва».* Дані нормативні акти на час свого введення в дію були дуже актуальними для структур, що займаються безпекою підприємництва, сприяли розвитку їх діяльності, оскільки давали змогу більш повно задовольнити запити їх замовників стосовно надійності потенційних партнерів. За оцінками експертів, *«в системі державного управління підприємництвом України створені сприятливі умови, що дозволяють розробити необхідну нормативну базу для цивілізованого надання послуг юридичним і фізичним особам у сфері забезпечення безпеки, а також організації господарюючими суб’єктами власних служб безпеки»*. Для розвитку правової бази, орієнтованої на створення умов для підвищення ефективності безпекових послуг для вітчизняного підприємництва, було прийнято й інші нормативні акти. Серед них закони *«Про оперативно- розшукову діяльність», «Про державну таємницю»* та ін. У т.ч. визначено поняття спеціальних технічних засобів як устаткування, апаратури, приладів, препаратів та інших виробів, спеціально виготовлених, розроблених, модернізованих, запрограмованих чи пристосованих для виконання завдань негласного одержання інформації під час здійснення оперативно-розшукової діяльності.

Застосування спеціальних технічних засобів в Україні дозволяється лише оперативним підрозділам, визначеним Законом України *«Про оперативно- розшукову діяльність».* Виключно для таких підрозділів дозволяється розробка, виготовлення і реалізація спеціальних технічних засобів.

Варто зауважити, що поряд із названими вище нормативними актами правову основу для діяльності недержавної системи безпеки підприємництва протягом останніх років було зміцнено низкою інших документів, пов’язаних із рішеннями органів державної влади у зв’язку із реалізацією програми боротьби зі злочинністю та організації безпеки підприємницької діяльності. Однак, динаміка суспільного життя, пов’язана із впливом глобальних процесів на українську дійсність, розвиток ринкових відносин, соціально-політичні фактори виводять питання організації безпеки національного підприємництва за участю недержавних структур, як приватних, так і громадських, в число найважливіших завдань сьогодення. Відповідно зростає і кількість проблем, правове врегулювання яких в кінцевому рахунку має сприяти зміцненню економічної безпеки України.

Практика безпекової діяльності в Україні засвідчила необхідність розширення послуг, пов’язаних також із охороною особи, її здоров’я, свободи, громадянських, майнових прав та ін. У зв’язку з цим назріла необхідність координації діяльності правоохоронних органів, спецслужб і недержавних структур безпеки, в т. ч. детективних. Ця точка зору об’єднує більшість експертів. Як зауважує Е. І. Низенко, *«за своїм характером детективна діяльність є гласною, але пов’язана із пошуковими діями та певними обмеженнями компетенції осіб, які її здійснюють. Тому одним із реальних кроків в напрямі розвитку детективної діяльності може стати розробка нормативної бази для здійснення даного виду підприємництва»*. Цим же автором обгрунтовано ставиться питання про необхідність правового регулювання підприємницької діяльності, пов’язаної із технічним і криптографічним захистом інформації. Він справедливо зауважує, що наявні з цього приводу документи орієнтовані на вузьке коло висококваліфікованих спеціалістів і малодоступні для всіх інших практиків. Щодо останніх малодоступними лишаються також і технічні засоби для фіксації аудіо – та відеоінформації стосовно протиправних дій, що теж є ще невирішеною проблемою для недержавних структур безпеки.

Протягом останніх 12 років проект Закону України «Про зброю» не раз виносився на розгляд Верховної Ради України різних скликань, але так і не був прийнятий. Основним каменем спотикання стали дебати навколо можливих наслідків прийняття даного законопроекту. Поширеними в усіх дебатах з цього приводу є побоювання, що володіння вогнепальною зброєю сприятиме зростанню злочинності. Тобто, приватним охоронцям, як зазначає О.Єрмоленко, *«залишають можливість боротися з озброєними злочинцями в рукопашну, прикриваючи «персон охорони» власними тілами»*.

Заслуговують на увагу й висновки президента Української Федерації працівників недержавних служб безпеки С.Шабовта, який порівнюючи російський ринок безпекових послуг з українським заявив, що в Росії існує державне регулювання ринку безпеки і є відповідна система законів. В той же час як в Україні немає жодного закону, що регулював би питання функціонування цього ринку. При цьому він пояснив, що мова йде про відсутність правового регулювання у сфері охоронної і детективної діяльності, захисту комерційної таємниці і т. ін.

Загалом, за результатами проведеного аналізу, з метою правового врегулювання правовідносин, пов’язаних з діяльністю недержавних суб’єктів сектору безпеки України вважається за необхідне:

1) розробити (чи доопрацювати раніше підготовлені законопроекти) та прийняти: – Закон України «Про внесення змін і доповнень до Закону України «Про основи національної безпеки», в якому більш чітко визначити можливість функціонування та роль недержавних суб’єктів сектору безпеки в системі забезпечення національної безпеки України; спеціальні закони «Про охоронну діяльність», «Про детективну діяльність», «Про зброю», «Про комерційну таємницю», «Про протиправне поглинання та захоплення підприємств» та «Про службу безпеки суб'єктів господарювання та інших юридичних осіб»;

2) розробити та прийняти «Загальнонаціональну програму організації безпеки підприємництва в Україні», а також відповідні акти Кабінету Міністрів України та інших центральних органів виконавчої влади;

3) опрацювати питання щодо систематизації та кодифікації законодавства у сфері національної безпеки та діяльності державних і недержавних суб’єктів сектору безпеки України. Реалізація зазначеного, за нашими оцінками, сприятиме формуванню належної правової бази для повноцінного функціонування системи захисту українського підприємництва та бізнесу від реальних і потенційних загроз в сучасних умовах глобалізації та світової економічної інтеграції.

**2. Суб’єкти недержавної правоохоронної діяльності та їх місце у забезпеченні безпеки підприємств.**

Внутрішній зміст поняття системи безпеки фірми є досить комплексним, містить ряд елементів, зокрема об'єкт та суб'єкт безпеки Об'єктом безпеки підприємства виступає все те, на що спрямовані зусилля щодо забезпечення безпеки, або ж те, що потребує захисту:

• кадровий персонал підприємства, а саме: керівний склад, акціонери, структурні підрозділи та їх співробітники, функції яких пов'язані з різними видами інформації;

• майновий, інтелектуальний та фінансовий капітал підприємства;

• притаманні специфіці фірми види фінансово-господарської діяльності підприємства.



Отже, об'єктом безпеки підприємства, передусім економічної, є вся система її повноцінного функціонування. Уразивши хоча б один із об'єктів безпеки підприємства, остання зазнає відповідного впливу на окрему ділянку фірми, що може обернутися небезпекою або загрозою втрати балансу рівноваги виробничо-господарського механізму підприємства. Кожне підприємство (суб'єкт господарювання) має як загальний об'єкт безпеки, так і специфічний, через особливості її діяльності.

Об'єктивно, на даний момент, в сфері забезпечення безпеки підприємництва в Україні, функціонують дві групи суб'єктів:

* держава, яка діє через органи законодавчої, виконавчої, судової влади, правоохоронні органи і спецслужби;
* недержавні організації в особі приватних охоронних підприємств, комерційних служб безпеки, служб безпеки банків, інформаційних та учбових центрів, вищих навчальних закладів, громадських організацій.

При цьому головними принципами, якими необхідно керуватись суб'єктам в процесі їх спільної діяльності по забезпеченню безпеки особистості і підприємництва, повинні стати:

* взаємна відповідальність державних і недержавних структур перед законом за дії, що наносять збитки національним інтересам, а також правам людини, її власності та діловій репутації;
* захист державою законних інтересів недержавних організацій у відповідних сферах їх діяльності;
* взаємодія в боротьбі з кримінальним сектором в економічній та фінансовій сферах діяльності;
* взаємодія в боротьбі з проявами екстремізму, тероризму, незаконного обігу наркотичних речовин та організованної злочинності в усіх сферах діяльності;
* надання пріоритетної допомоги недержавним організаціям, які приймають безпосередню участь в захисті безпеки найбільш важливих для держави підприємств;
* повага і дотримання прав і свобод людини і громадянина.

Суб'єктів безпеки підприємства можна класифікувати за такими ознаками:

Залежно від приналежності:

• власні служби безпеки, що входять у структуру суб'єктів господарювання і повністю утримуються за їхні кошти. Структура цих підрозділів базується залежно від рівня становлення фірми, масиву питань, вирішення яких покладає на ці служби керівництво підприємства на тому чи іншому етапі її розвитку;

• самостійні комерційні чи державні організації, що наймаються суб'єктом господарювання для виконання функцій щодо забезпечення окремих або всіх аспектів його безпеки. Такі суб'єкти як правило, спеціалізуються або на чисто режимно-охоронних послугах (охорона будівель, споруд, транспорту, окремих працівників підприємств, установ, членів їх сімей тощо), або на суто економічних, правових чи консультаційних послугах.

Залежно від безпосередньої участі у забезпеченні безпеки підприємства:

• спеціальні суб'єкти, створені виключно для виконання функцій щодо забезпечення безпеки фірми, як її власна служба безпеки, так і залучена на умовах договору;

• напівспеціальні суб'єкти, до безпосередніх функцій яких входить ряд таких, що спрямовані на забезпечення безпеки підприємства. Такими суб'єктами є відділ кадрів, фінансово-кредитний відділ, медична частина тощо;

• решта персоналу та структурні підрозділи, участь яких у здійсненні заходів щодо забезпечення безпеки підприємства має винятковий характер.

Залежно від форми власності та підпорядкування:

• державні органи — здійснюють повноваження щодо безпеки суб'єктів фінансово-господарської діяльності, до структури яких вони входять, або ж надають послуги стороннім фірмам на умовах укладених договорів, прикладом чого є діяльність. Державної служби охорони МВС України щодо заходів безпеки усіх без винятку комерційних банків в Україні;

• недержавні органи, які представлені охоронними організація ми, аналітичними центрами, інформаційними та консалтинговими службами, які за відповідну плату на умовах договор надають послуги щодо охорони об'єктів, здійснюють захист інформації, комерційної таємниці тощо. До цієї групи суб'єкті належать і власні служби безпеки підприємства недержавне форми власності.

Залежно від правової основи функціонування (легітимності суб'єктів:

• офіційні органи, що фунціонують у межах чинного законодавства України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України;

• не легітимні структури, діяльність яких відбувається поза правовим полем України. Наразі їх функціонування має динаміку до зменшення, що викликано відмовою суб'єктів бізнесу від їхніх "послуг", однак відкидати їх існування не варто. Зазначені суб'єкти, іншими словами "дах", пропонують свої послуги через погрози, насилля, погроми гарантуючи при цьому захищеність від подібних структур. Зазвичай такі послуги пропонуються суб'єктам бізнесу, діяльність яких повністю або частково відбувається в тіні, що є підставою до шантажу.

Перелік зазначених вище суб'єктів безпеки підприємства, крім останнього, успішно формує ринок послуг щодо забезпечення безпеки бізнесових структур. Найчастіше вітчизняні підприємці формують попит на фізичну охорону будівель, інкасацію, комплекс захисних заходів від рекету і прослуховування телефонних каналів зв'язку, приміщень від радіозакладок, комп'ютерів і комп'ютерних мереж від несанкціонованого проникнення та вірусів.

**3.Вимоги до працівників недержавних служб безпеки**

Одним із головних завдань соціальної та правової держави є забезпечення конституційних прав людини на захист своїх законних прав та інтересів. Виконання цього завдання відбувається шляхом створення системи правоохоронних органів. Проте діяльність лише державних правоохоронних органів не завжди здатна повною мірою забезпечити конституційне право людини на захист своїх законних прав та інтересів.

Отже, постає необхідність створення альтернативного недержавного правоохоронного механізму.

Сучасний світовий досвід свідчить про те, що чимало країн світу у забезпеченні правопорядку та безпеки покладаються не лише на державні правоохоронні органи, але й на недержавні суб'єкти правоохоронної діяльності. Частка працівників недержавних правоохоронних структур у ряді країн світу, зайнятих в індустрії забезпечення безпеки, коливається від 50 % до 80 % від загальної кількості осіб, професійно зайнятих боротьбою зі злочинністю.

Вимоги, що ставляться до кандидатів на роботу до служби безпеки фірми визначаються станом загроз і небезпек, специфікою діяльності фірми, а також політикою безпекозабезпечення, яка формується і реалізується на фірмі. Беручи до уваги організаційну структуру служби безпеки фірми, варто зазначити, що вимоги, які ставляться до її працівників дещо різняться, однак єдиними вони є з позиції проникнення розумом і відчуття серцем психології загальної справи, корпоративних інтересів, поваги до керівника, загалом сприймання роботи на фірмі, як частини свого життя. Тобто вимоги до працівників служби безпеки можна представити у формі *психофізіологічних, психологічних*та *фізичних.*Зупинимося на їх характеристиці.

*Психофізіологічні вимоги*передбачають уміння працівника швидко реагувати на зміну ситуації, бути уважним і спостережливим, безпомилково орієнтуватися у просторі, мати скоординовані рухи, а також вміння виявляти головне з-поміж різного та приймати рішення незважаючи на втому, емоційний стан та стресову ситуацію.

*Психологічні вимоги*до працівників полягають у наявності середньостатистичного інтелектуального розвитку, гарної манери поведінки, здатності мислити, сприймати та опановувати нові знання та практичні навички, бути самокритичним і неупередженим у ставленні до інших, прогнозувати ситуацію та можливий результат шляхом поетапного досягнення успіху, бути відданим професії, тримати в таємниці все, що стало відомо у процесі роботи тощо. Проблеми в роботі служби можуть створити працівники з вразливим характером, дратівливі, образливі, авантюрні, заздрісні, балакучі, безініціативні, без належного такту, самозакохані, такі, що надто люблять розваги й красиве життя, жінок, гроші та славу.

Саме тому одним із засобів, що суттєво знижує ймовірність кадрової помилки з кандидатом на роботу до служби безпеки фірми, є застосування поліграфів. Зазвичай проводять три основних *види перевірок*із використанням поліграфу:

- скрінінгові перевірки при відборі кадрів на роботу, які виявляють для працедавця справжні мотиви працевлаштування, наявність алкогольної і наркотичної залежності, судимості та зв'язків із кримінальними елементами, інформацію про нанесення фінансових і матеріальних збитків підприємствам, установам, організаціям, на яких працювала дана особа, інформацію про крадіжки на попередніх місцях роботи, фальсифікування анкетних даних тощо. Ті фірми чи установи, що використовують детектор брехні, значно зменшують витрати, пов'язані з крадіжками продукції та готівкових грошей, витоком конфіденційної інформації, високою плинністю кадрів, низькою продуктивністю праці, а загалом забезпечують собі формування сприятливого клімату у колективі;

періодичні перевірки працюючого персоналу, що є актуальним і важливим завданням вищого менеджменту будь-якої компанії, адже люди змінюються і треба вчасно помітити ці зміни. Чим більш прибутковим є бізнес, тим жорстокішою є конкуренція, тим більше шансів, що конкурентна боротьба перестане бути теоретичною. Шкоду, яку може завдати організації нелояльний працівник, тим паче служби безпеки фірми, що наділений владою, важко підрахувати;

- перевірки персоналу фірми в ході службових розслідувань, що дають можливість підтвердити або ж спростувати думки про зраду інтересів фірми.

Як свідчать статистичні дані, збитки компаній та корпорацій від злочинів і зловживань їх співробітників вражають уяву. Так, у травні 2005 р. у США був зареєстрований найбільший витік банківської інформації приватного характеру. Жертвами групи зрадливих працівників стали чотири великі банки і майже 700 тис. фізичних клієнтів. Збитки від розкрадання з боку власного персоналу компаній у США і Європі сягають 6-9% річного обороту. Не ліпші справи і в вітчизняних суб'єктів бізнесу, хоча такі дані не розголошуються.

*Фізичні вимоги*передбачають недопущення до роботи у службі працівників зі слабким фізичним здоров'ям, наявністю хронічних хвороб, схильних до наркотиків та алкоголю. Однак це не означає, що кожен працівник повинен мати спортивний розряд із боротьби, боксу, стрільби тощо, важливіше, щоб працівник постійно покращував свій фізичний стан постійними тренуваннями, а не тішився славою свого спортивного минулого. Адже наявність спортивних заслуг охоронця - це не щит від вогнепальної зброї, яка дає змогу не вступати у контакт з об'єктом та його охороною. Більше того, у поєдинок із нападниками охоронцю доводиться вступати не на рингу, а, як правило, при скупченні людей. І наостанок, поєдинок охоронців із нападниками є свідченням невисокого рівня організації охорони об'єкта.

Як відмічають вітчизняні вчені С. І. Ніколаюк та Д. Й. Никифорчук, для особистої охорони більш цінні такі працівники, які не відрізняються ні зовнішністю, ні одягом, ні поведінкою. Важливіше, щоб захисники мали голову на плечах і вміли нею користуватися, адже їх головне завдання полягає не в тому, щоб затуляти об'єкт від куль своїм тілом, а в запобіганні екстремальних ситуацій та в миттєвих, але цілеспрямованих і грамотних діях, якщо така ситуація виникає.

Не варто також, на думку вчених, акцентувати кадрову політику на осіб, що пройшли Афганістан, Боснію чи Чечню, або, принаймні, службу у спецназі чи десантних військах. Хоча багато людей вважає, що ті, хто пройшов крізь «м'ясорубку» справжньої війни, отримали колосальне психологічне загартування. Це правильно лише щодо тих, хто пішов на війну, маючи відповідну підготовку і впевненість у потребі його особистої участі в ній. Таких, як відомо, було небагато, і вони, як правило, не наймаються охоронцями. Скоріше, вони можуть стати найманими вбивцями. В інших військовий досвід призводить до алкоголізму, наркоманії, неврозів, депресії. Немало й таких, у кого «їде дах». Варто зазначити, що особиста охорона американських бізнесменів ніколи не формувалася з колишніх морських піхотинців, що пройшли через В'єтнам, хоча такі варіанти мають місце у кінобойовиках.

Викликає сумнів також твердження, що найкращими охоронцями є колишні співробітники оперативних підрозділів правоохоронних органів (СБУ, МВС України). Так, справді, їх професійний досвід та підготовка близькі до того, що потрібно тілоохоронцю (навички спостереження, відкритого стеження, захвату злочинців, стрільби, керування автомобілем тощо). До того ж, у них зберігаються зв'язки з колишніми співробітниками. Однак деякі колишні навички можуть виявитися в особистій охороні шкідливими, наприклад, звичка робити застережний постріл у повітря. І ще важче звикнути до роботи в умовах правового свавілля. Так, зброю тілоохоронець (якщо він має дозвіл на неї) може використати, як і всі громадяни, лише в разі потрібної оборони. Допитувати затриманих він не має ніякого права, бо він, відповідно до закону, є приватною особою. Заходи фізичного впливу з метою захисту клієнта можна кваліфікувати, як злісне хуліганство, а переслідування злочинця - як порушення недоторканності житла, вторгнення в особисте життя громадян тощо.

Отже, вимоги, що пред'являються до кандидатів на роботу до служби безпеки фірми, дають можливість лише створити певний бар'єр у працевлаштуванні на фірму. Поза тим вибір найкращого кандидата з-поміж багатьох - це справа керівника. Корисно лише пам'ятати: ціна помилки при прийманні на роботу величезна, адже ці помилки тягнуть за собою значні людські та фінансові втрати. Причому витрати зростають прямо пропорційно зростанню обсягів відповідальності, що покладається на працівника служби безпеки. Чим вищий у нього ранг (посада), тим більшими втратами обійдеться кадрова помилка. Якщо працівник входить до вищого керівництва фірми, то наслідки можуть бути особливо руйнівними для фірми і навіть коштувати їй «життя». Очевидні втрати непродуманого найму включають у себе даремно виплачену зарплату, витрати на навчання, виплати компенсацій, пов'язані з достроковим припиненням контракту, витрати на пошук нових працівників. Але найбільші втрати важко зразу ж побачити й оцінити, адже вони включають в себе стратегічні прорахунки й управлінські помилки, допущені працівником, втрачені можливості, додатковий стрес і зіпсовані стосунки на фірмі.

Задля недопущення подібного, приймаючи на роботу нового співробітника служби безпеки фірми, варто діяти неквапно й обережно. Чим вища посада й зарплата, тим більше часу потрібно на прийняття рішення. Не варто намагатися якомога швидше вирішити кадрове питання, адже неправильний вибір лише погіршить ситуацію на фірмі. Варто проглянути якомога більше кандидатів і провести з ними співбесіди; треба ретельно вивчити рекомендації, перевірити знання претендентів за допомогою тестів. Доцільно також звернутися за допомогою до досвідчених консультантів, яким керівництво фірми довіряє. Не зайвим також буде поговорити з тими, хто працював чи працює разом із кандидатом, а також поспостерігати за ним під час обіду або під час його бесіди з іншими людьми.

Варто критично поставитися до інформації про колишні невдачі претендента; можливо, фірма, де він працював, пригнічувала його можливості; до відомостей про його колишні успіхи: можливо, він досяг їх лише завдяки фірмі, в якій працював.

Не варто також ігнорувати особисту інтуїцію. Якщо стосовно кандидата щось бентежить, то можливо з ним справді не все гаразд. Варто прислухатись і до думки перевірених радників. І лише тоді можна приймати рішення. Однак варто пам'ятати, що ніхто не може знати, чи правильну людину прийняли на фірму, допоки вона себе сама не покаже у роботі.

Якщо ж все ж таки «закралася помилка» у кадровій роботі, прийнявши на роботу не ту людину, то треба негайно виправити помилку, адже ціна помилки з часом не стане нижчою. При цьому для звільнення працівника з роботи існує багато причин. Наприклад:

- не підходить для роботи у службі безпеки фірми;

- хронічно не вміє працювати з новими обов'язками або ставиться до роботи несерйозно;

- відсутній потрібний досвід чи здатність навчатися новому і встигати за мінливим світом;

- некомунікабельність, тобто невміння спілкуватися з колегами та клієнтами.

У всякому разі, коли стає зрозумілим, що працівника варто звільнити, треба це зробити якомога швидше. Керівник при цьому мусить діяти згідно з законом, дотримуючись усіх правил і процедур, діючи з тією відповідальністю, що лягає на нього, і хоч як би важко не було, він повинен зробити все те, що треба зробити.

Дещо інша ситуація, коли працівник неретельний, некерований, непрацелюбний, і про це знає весь колектив. Тому в такому разі, чим довше приймається рішення про звільнення, тим більше працівники будуть сумніватися в компетенції свого керівника. Адже добрий керівник звільняє, довго не роздумуючи, оскільки так краще і для працівника, якого звільняють, і для інших працівників, і для фірми, і для клієнтів та партнерів, й для нього самого. Почасту співробітник, над яким «згустилися хмари», відчуває це, а тому швидке звільнення розрядить напруження на фірмі.

Практика функціонування служб безпеки фірм та політика їх кадрового менеджменту дає підстави ставитися з пересторогою або ж не мати справи з працівниками, які не відповідають зазначеним вимогам. Тому шляхом проведення іспитів, психологічного тестування, співбесід, вивчення біографії та поданого резюме, доручення незначних завдань, проведення гласної і негласної перевірки, ознайомлення з думками товаришів і колег за попереднім місцем роботи можна сформувати чітке уявлення про майбутнього працівника служби безпеки фірми.

Підсумовуючи викладене, варто ще раз наголосити: ринкова економіка є складним соціальним середовищем, в якому виживає сильніший і захищеніший

**Тема 5. Система безпеки підприємства та її створення**

План.

Вступ.

1. Створення на підприємстві системи безпеки та її структура
2. Основні функції служби безпеки підприємств
3. Права та обов’язки працівника СБП

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

**Вступ**

На нашу думку у створенні системи безпеки бізнесу, в першу чергу, мають бути зацікавлені власники та менеджмент приватних підприємств, компаній тощо. Адже саме вони приймають рішення про розвиток бізнесу та фінансування його безпеки. Вони повинні ставитися до цього процесу відповідально і продумувати способи попередження загроз підприємству, окремим його підрозділам чи співробітникам, підприємницькій діяльності в цілому. Захистом бізнесу  на підприємствах сьогодні займаються служби безпеки, що опікуються цими проблемами. Треба розуміти, що наразі не існує єдиного підходу до поняття системи безпеки підприємства. Її методологія  та практична основа роботи індивідуальна для кожного господарюючого суб’єкта і полягає  в розробленні власної концепції безпеки підприємства.

Ця концепція мусить відповідати на такі питання:

- хто (що) саме потребує захисту;

- які загрози та підстави для них можуть з’явитися під час діяльності підприємства;

- хто саме і яким чином захищатиме підприємство задля його безпеки;

- які системні та екстрені заходи слід вживати задля  безпеки функціонування підприємства.

Для того, щоб концепція працювала ефективно, це мають бути прості та чіткі описи та інструкції що робити в тій чи іншій ситуації, прийоми та методи втілення концепції в практику. Ці документи повинні враховувати не лише явні, а скриті загрози бізнесу, рекомендації для персоналу щодо дій в умовах, які не були передбачені концепцією.

* 1. **Створення на підприємстві системи безпеки та її структура**

Для створення служби безпеки керівництво і менеджери насамперед розпочати створення її системи безпеки, визначити структурні варіанти іі перспективи її розвитку. Але передусім треба визначити можливості:

* використання служб охорони за контрактом;
* створення власної служби безпеки;
* залучення допомоги державних служб охорони;
* протидії загрозам з боку терористів;
* протидії загрозам вибухів, комп'ютерним злочинам;
* протидії "білокомірцевій" злочинності;
* використання спецтехніки (відео - та інших оперативних систем охорони різних суб'єктів і об'єктів, спеціальних технічних засобів охорони периметра об'єкта, систем охоронного устаткування і центрального управління і т.ін.)

Вирішити створити власну службу безпеки, підприємець передусім повинен звернутися до експертів у галузі організації сучасної системи безпеки недержавного підприємства з проханням провести дослідження цієї проблеми і підготувати пакет документів, що визначають програму і функціонування системи безпеки підприємства. Краще за все це можуть зробити професійно підготовлені менеджери безпеки.

Чому потрібно створювати систему безпеки навіть у малому й середньому бізнесі, зрозуміли вже багато підприємців. В умовах сучасної України для господарюючого суб'єкта існують такі основні джерела загроз, небезпек, втрат, конфліктів і ризиків:

* розкрадання (крадіжки) фондів, власності, дрібні крадіжки, що здійснюються співробітниками;
* "білокомірцева" злочинність, корупція;
* комп'ютерна злочинність, загрози технічного проникнення і просочування електронної інформації;
* вандалізм, вибухи, пожежі, підпали;
* викрадення, захоплення заручників, рекет, загрози шантажу;
* загрози природного походження (катаклізми);
* масові безпорядки.

У процесі організації комплексної системи безпеки господарюючого об'єкта особливу увагу слід звертати на такі елементи:

* здатність розробити програму, адекватну специфічним потребам захисту об'єкта;
* ступінь надійності працівників підприємства;
* вартість програми захисту об'єкта;
* ступінь надійності захисту об'єкта;
* достатня ефективність витрат на програму діяльності;
* рівень загальної відповідальності адміністрації;
* здатність програм гарантування безпеки відповідати вимогам;
* страхові премії як результат виконання програми;
* здатність модернізувати систему безпеки відповідно до сучасних вимог;
* здатність прищепити працівниками підприємства відчуття корпоративності;
* надійність виробника спеціального обладнання, яке використовується для захисту об'єкта;
* засоби впливу на громадську думку на користь вирішення проблем безпеки об'єкта.

Для ефективного функціонування служби безпеки потрібно попередньо опрацювати багато питань. Серед них особливе значення має проектування оргструктури служби безпеки та її ресурсного забезпечення, оскільки без вирішення цих питань її діяльність взагалі неможлива.

Серед причин нерівномірні кількості працівників у різних підрозділах служби безпеки можна назвати фінансові можливості підприємства-засновника, наявність або відсутність таємниць, що охороняються, ступінь участі у конкурентній боротьбі і т.ін. Кожен підрозділ служби безпеки має свої специфічні цілі, завдання і функції, реалізація яких (оскільки вони взаємно доповнюють одне одного) дає змогу значно підвищити ефективність служби безпеки в цілому.

В організаційній структурі передбачена також посада керівника служби безпеки, яка на практиці трансформувалася в начальника служби безпеки. Очевидно, що коли персонал служби безпеки за чисельністю великий, неминуче виникає питання щодо заступників начальника служби безпеки. їх також має бути не менше трьох - за кількістю підрозділів служби безпеки.

Будь-яка оргструктура, навіть най оптимальніша, не зможе дати очікуваних результатів, якщо її не доповнити внутрішніми нормативними актами, що регулюють діяльність усіх підрозділів і співробітників служби безпеки. Образно кажучи, "кістка" (оргструктура) має обрости "м'ясом" (нормативними документами). Причому ці нормативні акти умовно можна поділити на дві групи:

1) ті, що безпосередньо стосуються діяльності самої служби безпеки;

2) ті, що регулюють діяльність інших служб (підрозділів, працівників) підприємства.

До *першої групи належать*: статут служби безпеки, положення про відділи і штаб служби безпеки, положення про групи і сектори служби безпеки, посадові інструкції працівників служби безпеки.

Структура посадової інструкції має такі розділи: загальні положення; функції; посадові обов'язки; відповідальність; взаємини і зв'язки за посадою. Розробляють ці нормативні акти послідовно, починаючи із статуту до посадової інструкції, що дає змогу охопити весь комплекс цілей, завдань і функцій, що вирішуються службою безпеки.

До *другої групи* внутрішніх нормативних актів, що забезпечують діяльність інших працівників і служб підрозділів підприємства-засновника, належать:

* договір підприємства з партнером про забезпечення ним заходів безпеки комерційної інформації;
* інструкція щодо виконавців робіт і документів, що містять комерційну таємницю;
* зобов'язання про нерозголошення комерційної таємниці;
* перелік відомостей, що становлять комерційну таємницю підприємства і основні вимоги до працівників з її захисту;
* перелік відомостей, які не повинні розголошуватися стороннім особам з метою особистої безпеки працівників підприємства;
* перелік посадових осіб, уповноважених відносити інформацію до комерційної таємниці;
* правила віднесення інформації до комерційної таємниці і зняття з її носіїв грифу конфіденційності;
* правила ведення таємного діловодства;
* пам'ятка працівникові (службовцеві) про збереження комерційної таємниці підприємства;
* правила приймання відвідувачів на підприємстві;
* правила внутрішнього трудового розпорядку і т.ін.

Проте оптимальна оргструктура і повне правове забезпечення служби безпеки самі по собі не забезпечать її ефективного функціонування, якщо вона не матиме відповідних ресурсів. Продовжуючи образні порівняння, можна стверджувати, що після того, як "кістка" (оргструктура) обросла "м'ясом" (внутрішні нормативні документи), слід поклопотатися про "їжу" (ресурси). Серед них першочергове значення мають фінансові ресурси. Без фінансового забезпечення діяльності служби безпеки безглуздо взагалі говорити про її функціонування.

* 1. **Основні функціі служби безпеки підприємств**

Завдання гарантування безпеки підприємства є одним із основних, пріоритетних завдань, що стоять перед усіма структурними ланками і всіма працівниками підприємства, так само як і завдання збільшення прибутку, підвищення власного добробуту. Ефективний захист економічних інтересів фірми може бути забезпечений лише у разі об'єднання зусиль її персоналу: адміністрації, інженерно-технічних працівників, службовців, робітників.

Служба безпеки підприємства - це самостійний структурний підрозділ. Вона вирішує завдання безпосереднього забезпечення захисту життєво важливих інтересів фірми в умовах комерційного і підприємницького ризику, конкурентної боротьби. На всіх великих і середніх підприємствах (в організаціях) звичайно створюються автономні служби безпеки, а безпеку функціонування невеликих фірм можуть гарантувати територіальні (районні або міські) служби за договорами найму одного чи кількох охоронців. Такі служби охорони зазвичай створюються при місцевих органах внутрішніх справ або при державній службі безпеки.

Основною метою підсистеми безпеки фірми є запобігання: збитку в її діяльності за рахунок розголошення, просочування інформації та несанкціонованого доступу до джерел конфіденційної інформації; розкраданню фінансових і матеріально-технічних коштів, знищенню майна і цінностей; порушенню роботи технічних засобів забезпечення виробничої діяльності, зокрема засобів інформатизації, а також запобігання збитку персоналу організації. Завданнями підсистеми безпеки підприємства є:

* своєчасне виявлення й усунення загроз персоналу і ресурсам; причин і умов виникнення фінансового, матеріального і морального збитку інтересам фірми, порушення її нормального функціонування і розвитку;
* віднесення інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації, належного захисту від неправомірного використання), а інших ресурсів - до різних рівнів уразливості (небезпеки) і до категорії тих, що підлягають збереженню;
* створення механізму і умов оперативного реагування на загрози безпеки і прояви негативних тенденцій у функціонуванні фірми;
* ефективне припинення посягань на ресурси і загроз персоналу на основі комплексного підходу до безпеки;
* створення умов для максимально можливого відшкодування й локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, для ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічної мети.

Організаційна структура підсистеми безпеки організації може бути різною залежно від виду підприємства (банк, фірма), його розмірів, форм власності тощо. Створювати її слід усвідомлено й раціонально, максимально використовуючи досвід фахівців у сфері безпеки бізнесу.

Структура, чисельність і склад служби безпеки визначаються реальними потребами фірми і ступенем конфіденційності її інформації. Залежно від розмірів і потужності організації її безпека і захист інформації можуть бути гарантовані по-різному: від абонементного обслуговування силами приватних охоронних і детективних структур до розгортання повномасштабної власної служби і системи безпеки з розвиненою структурою і штатною чисельністю

Служба безпеки підприємства завжди має бути готовою до подолання критичної (кризової) ситуації, що може виникнути через зіткнення інтересів бізнесу та злочинного світу. Для управління безпекою багато які фірми створюють так звані кризові групи, у складі яких працюють керівник фірми, юрист, фінансист і керівник служби безпеки. Головна мета діяльності кризової групи - протидіяти зовнішнім загрозам для безпеки підприємства.

Служба безпеки будь-якої підприємства постійно виконує певний комплекс завдань. Головними з них для будь-якої фірми є такі:

1) гарантування безпеки виробничо-господарської діяльності та захисту відомостей, що вважаються комерційною таємницею фірми (підприємства, організації);

2) організація роботи з правового та інженерно-технічного захисту комерційної таємниці фірми;

3) запобігання необґрунтованому допуску й доступу до відомостей та робіт, які становлять комерційну таємницю;

4) організація спеціального діловодства, яке унеможливлює несанкціоноване одержання відомостей, віднесених до комерційної таємниці відповідної фірми;

5) виявлення і локалізація можливих каналів витоку конфіденційної інформації в процесі звичайної діяльності та в екстремальних ситуаціях;

6) забезпечення режиму безпеки за здійснення всіх видів діяльності, зокрема зустрічі, переговори й наради у рамках ділової співпраці фірми з іншими партнерами;

7) забезпечення охорони приміщень, устаткування, офісів, продукції і технічних засобів, необхідних для виробничої або іншої діяльності;

8) забезпечення особистої безпеки керівництва та провідних менеджерів і спеціалістів фірми;

9) оцінка маркетингових ситуацій та неправомірних дій конкурентів і зловмисників.

Зрозуміло, що перелік конкретних завдань щодо гарантування безпеки фірми залежно від специфіки її діяльності може бути більшим або меншим, але завжди достатнім та обґрунтованим

* 1. **Права та обов’язки працівника СБП**.

**Тема 6.** **Розробка концепції і впровадження системи безпеки підприємства**

План

Вступ

1. Вимоги до концепції безпеки підприємства.

2. Структурна модель рівнів діяльності підприємства (організації, функціонування і прийняття рішень).

3. Методологічні засади концепції безпеки підприємства.

4. Організаційні аспекти діяльності аналітико-інформаційної служби підприємства.

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

**Вступ**

У житті сучасного суб'єкта підприємницької діяльності питаннями забезпечення охорони й безпеки управлінських і виробничих процесів займається служба безпеки даного підприємства, а методологічною й практичною основою її діяльності є концепція безпеки підприємства.

**1.Вимоги до концепції безпеки підприємства.**

Взагалі, концепція безпеки підприємства повинна відповідати на декілька дуже простих питань:

* які особи і які об'єкти потребують захисту;
* які загрози можуть виникнути в процесі функціонування підприємства;
* хто і як буде захищати підприємство від загроз, що виникли щодо його безпеки;
* які системи необхідно задіяти для забезпечення безпеки процесів життєдіяльності підприємства і як вони повинні функціонувати.

На практиці, концепція безпеки підприємства найчастіше містить аналіз і рекомендації до дії та протидії впливу наступних несприятливих факторів:

* група загроз кримінального й терористичного характеру (у т.ч. фізичний захист від впливу вуличної й організованої злочинності, захист від вимагання, шахрайства, інших протиправних дій);
* група загроз інформаційної й підприємницької безпеки підприємства (у т.ч. підтримка певного рівня таємності документів, комп'ютерних даних, комунікацій, протидія агентурній діяльності серед персоналу організації);
* група загроз безпеки підприємства (у т.ч. охорона комерційної таємниці й захист інтересів підприємства в конкурентному середовищі);
* група загроз стихійного походження (у т.ч. виникнення надзвичайних ситуацій техногенного характеру, стихійних лих, інших форс-мажорних ситуацій).

Кожна концепція безпеки підприємства індивідуальна, оскільки повинна відображати індивідуальні особливості захисту діяльності саме цих конкретних об'єктів і суб'єктів, забезпечувати безпеку кожної складової підприємства, а також безпеку підприємства в цілому. Особливістю грамотної концепції безпеки є чітка методологічна основа, завдяки якій робота із забезпечення безпеки підприємства може бути формалізована до рівня чітких інструкцій, опису прийомів і методів. При цьому дані інструкції повинні передбачати не тільки методи протидії явним і очевидним погрозам, але й носити рекомендації для персоналу і їх реакцію на вплив небезпечних факторів, виникнення яких малоймовірно або взагалі не передбачалося концепцією.

1. **Структурна модель рівнів діяльності підприємства (організації, функціонування і прийняття рішень)**

Для того щоб уникнути кризових явищ, топ-менеджмент має здійснювати ефективне керівництво процесом розвитку підприємства, насамперед через систему управління, створюючи ефективну організаційну структуру.

Організаційна структура управління підприємством є засобом сприяння досягнення менеджерами своїх цілей. Оскільки цілі є похідними від загальної стратегії підприємства, тісний зв'язок стратегії та структури цілком логічний. Відповідно організаційна структура має дотримуватися певної стратегії. І якщо менеджери здійснюють вагомі зміни у своїй організаційній стратегії, вони мають модифікувати організаційну структуру задля пристосування до цих змін та їх підтримання. Відповідно до організаційної структури підприємства розробляється система управління підприємством.

З часом організаційна структура і система управління підприємством можуть зазнавати певних змін. Припускаючи, що процес розвитку організаційної структури є циклічним, можна виділити в її розвитку три фази: рівноваги; дисгармонії та зміни. На першій фазі організаційна структура управління відповідає за змістом та формою потребам підприємства. На другій фазі спочатку непомітно, а далі все суттєвіше простежується дисбаланс міх фактичним і необхіднім станом системи під впливом активно діючих внутрішніх та зовнішніх чинників. Застосовуючи відповідний набір методів управління, система на третьому етапі, фазі змін переводиться з розбалансованого стану в стан рівноваги.

*Організаційна структура управління підприємством* - основа системи управління, яка визначає склад, підпорядкованість та взаємодію її елементів окреслює необхідну кількість управлінського персоналу, здійснює його розподіл за підрозділами, регламентує адміністративні, функціональні та інформаційні взаємовідносини між працівниками апарату управління та підрозділами, встановлює права, обов'язки і відповідальність менеджерів тощо.

Зв'язки між елементами системи управління, які визначають відповідний тип організаційної системи управління підприємством, поділяють на:

- лінійні - виникають між підрозділами та керівниками різних рівнів управління і передбачають підпорядкованість одного керівника іншому;

- функціональні - характеризують взаємодію керівників, які виконують певні функції на різних рівнях управління, проте між ними не існує адміністративного підпорядкування;

- міжфункціональні - мають місце між підрозділами одного рівня управління.

Для відображення структурних взаємозв'язків основних рівнів та підрозділів підприємства, їх підпорядкованості на практиці використовують певні схеми організаційної структури управління. Такі схеми є лише скелетом системи управління, оскільки не розкривають склад та зміст функцій, прав та обов'язків підрозділів та посадових осіб.

*Типи організаційних структур управління підприємством*

Залежно від існуючих зв'язків між елементами системи управління виділяють лінійну, функціональну, лінійно-функціональну, дивізійну, матричну організаційні структури та ін.

Підприємства виникають як організації з простою структурою. У плануванні організації відображається її власник у ролі президента з усіма службовцями, які безпосередньо йому підпорядковуються. Проста (лінійна) структура визначається не наявністю, а відсутністю в ній будь-яких характеристик. Маємо низький рівень спеціалізації, нечисленні правила, за якими здійснюється діяльність, та централізацію повноважень у руках однієї особи - власника. Проста організація є "малоступеневою". Вона переважно складається з двох-трьох вертикальних рівнів та аморфної групи уповноважених службовців, які мають право централізовано приймати рішення. Проста структура найчастіше зустрічається у малому бізнесі, де менеджер і власник виступають в одній особі. Вона мобільна, потребує незначних витрат. Зі зростанням розмірів підприємства процес прийняття рішень ускладнюється, проста структура втрачає переваги, оскільки обмеженість її можливостей призводить до переобтяження керівної верхівки.

Правила простої структури поступаються більш формалізованим правилам зі зростанням обсягів виробництва або продажу, зі збільшенням чисельності працівників та управлінського персоналу. В цьому випадку формуються нові рівні менеджменту для координування діяльності підприємства. З функціонального і товарного способів департаменталізації постали дві найпопулярніші версії бюрократичного планування, які називають функціональною та дивізіональною структурами відповідно.

*Функціональна організаційна структура управління*

Передбачає поділ функцій управління між окремими підрозділами апарату управління. При цьому кожний виробничий підрозділ одержує розпорядження одночасно від кількох керівників функціональних відділів. Функціональна структура розширює функціональну орієнтацію, роблячи її панівною формою для підприємства. Переваги функціональної структури виникають унаслідок спеціалізації праці. Об'єднання подібних спеціальностей дає змогу заощадити витрати на масштабах, мінімізує дублювання функцій персоналу та устаткування і забезпечує службовцям комфорт і задоволення, оскільки дає їм змогу розмовляти "тією мовою, що й їхні колеги". Серед головних недоліків функціональної системи те, що в гонитві за функціональними цілями підприємство часто забуває про свої найголовніші інтереси. Цілковиту відповідальність можна покласти на якийсь один відділ, отже службовці окремих відділів ізолюються від інших і погано розуміються на обов'язках працівників інших відділів.

*Дивізійна організаційна структура управління*

Це структура, що складається з самодостатніх відділів або підрозділів. Спираючись на товарну департаменталізацію, кожний підрозділ загалом зберігає самостійність, за якою його менеджер відповідає за результативність і має цілковите право приймати стратегічні та поточні рішення. За цією системою управління лише стратегічні функції управління здійснюються централізовано на корпоративному рівні, а кожен виробничий підрозділ має власну розгалужену структуру управління, яка забезпечує автономне його функціонування.

Головною перевагою дивізійної структури є її орієнтація на результати. Менеджери підрозділів цілковито відповідають за вироблену продукцію. Крім того дивізійна структура звільняє персонал центрального офісу від повсякденних виробничих деталей, а отже, вони можуть приділити увагу довгостроковому та стратегічному плануванню.

Головний недолік дивізійної структури - дублювання діяльності та ресурсів. Наприклад, кожний підрозділ може мати відділ маркетингових досліджень. За відсутності самостійних підрозділів усі маркетингові дослідження підприємства можуть централізуватися й викопуватися коштом тих витрат, яких потребує дивізіоналізація.

Лінійно-функціональна організаційна структура управління передбачає розподіл повноважень і відповідальності за функціями управління й прийняття рішень по вертикалі. При цьому управління організоване за лінійною схемою, а функціональні підрозділи апарату управління допомагають лінійним керівникам вирішувати управлінські завдання.

*Лінійно-функціональна структура управління*

Матрична організаційна структура управління. Якщо функціональна структура пропонує переваги, які дістаються від спеціалізації, дивізійна структура більше зосереджується на результатах, однак втрачає від дублювання діяльності та ресурсів, то матрична структура поєднує переваги функціональної спеціалізації із зосередженістю та відповідальністю, які надає товарна департаменталізація. Поряд із лінійними керівниками підприємства і раціональним апаратом управління за матричної структури формують ще й тимчасові проектні групи.

Унікальною характеристикою матриці є те, що службовці в Цій структурі мають принаймні двох начальників: менеджера функціонального відділу та менеджера відділу продукції або керівника проекту. Останній здійснює керівництво функціональними службовцями, які є частиною групи менеджера проекту, однак повноваження розподіляються між обома менеджерами. Менеджер проекту переважно здійснює керівництво

*Матрична організаційна структура управління*

службовцями групи проекту в тому, що стосується цілей проекту, проте рішення щодо просування по службі, рекомендованої заробітної плати і щорічного перегляду цих даних залишаються прерогативою менеджера функціонального відділу. Задля ефективної праці менеджер проекту і менеджер функціонального відділу мають регулярно спілкуватися й координувати вимоги до своїх спільних підлеглих.

Перевага матриці полягає насамперед в здатності сприяти координації неоднорідного комплексу складних і взаємопов'язаних проектів та водночас дотримуватись економії, одержаної завдяки згрупуванню функціональних фахівців. Головні вади матриці - створювана нею плутанина та її схильність загострювати боротьбу за владу. Позбувшись послідовного керівництва, істотно поглиблюється двозначність. Плутанину спричинює нерозуміння того, хто перед ким звітуватиме. Відповідно, така плутанина і двозначність породжують боротьбу за владу.

Групова структура.

За умов використання групової структури підприємство утворюють робочі групи або команди, які здійснюють його діяльність. Члени команди мають повноваження ухвалювати рішення, які позначатимуться на них, оскільки в такому робочому середовищі не буває чіткої послідовності керівництва.

Організація без кордонів.

Цей тип організації управління підприємством не обмежується рамками або категоріями, нав'язуваними традиційними структурами, він стирає історичні кордони навколо підприємства, посилюючи його залежність від зовнішнього середовища. Замість створення функціональних спеціальностей, зосереджених у відділах, які виконують окремі завдання, у цій структурі згруповують службовців для набуття певних базових знань. Організації без кордонів - це малоступеневі компанії, які намагаються усунути вертикальні, горизонтальні та міжорганізаційні бар'єри. Появі таких організацій, які можуть швидко реагувати на зміни в зовнішньому середовищі і пристосовуватися до нього, сприяли глобалізація ринків і конкурентів, зміни в технології тощо.

Організаційна структура управління підприємством має забезпечувати ефективний процес прийняття рішень. Проте на підприємствах, на яких власність відокремлена від функцій управління, з метою збалансування інтересів власників і менеджерів та здійснення контролю з боку власників за діяльністю менеджерів виникає необхідність у формуванні додаткових органів управління (в доповнення до виконавчих органів), через які мають бути реалізовані інтереси власників підприємства щодо процедури прийняття рішень і здійснення управління підприємством. Для акціонерних товариств, зокрема, такими органами є загальні збори, спостережна рада і ревізійна комісія. Розробляючи організаційну структуру управління підприємством, його менеджмент має орієнтуватися на виробничу доцільність та законодавчі акти, які регламентують склад органів управління для підприємств, що створюються в організаційно-правовій формі господарських товариств.

Відповідно до Господарського кодексу України власник підприємства здійснює свої права щодо управління підприємством безпосередньо або через уповноважені ним органи відповідно до статуту підприємства чи інших установчих документів. Для керівництва господарською діяльністю власник (власники) або уповноважений ним орган призначає (обирає) керівника підприємства. На всіх підприємствах, які використовують найману працю, між власником або уповноваженим ним органом і трудовим колективом повинен укладатися колективний договір, який регулює виробничі, трудові та соціальні відносини трудового колективу з адміністрацією підприємства.

1. **Методологічні засади концепції безпеки підприємства**

Розробка концепції безпеки підприємства є підсумком ретельного аналітичного дослідження, а формування вичерпних і точних рекомендацій з роботи служби безпеки даного підприємства неможливо без серйозного досвіду багаторічної роботи в цій сфері. Фахівці нашого ПОС здатні виконати дану роботу на високо професійному рівні, здобуту під час служби в правоохоронних органах СБУ, МВС і підкріплену практикою діяльності щодо забезпеченню безпеки комерційних підприємств.

У ході розробки концепції безпеки підприємства, фахівцями нашої компанії проводяться наступні роботи:

• аналіз існуючих і можливих негативних факторів, що загрожують безпеки підприємства;

• створення служби безпеки підприємства, або аудит існуючої системи безпеки (з наданням звіту з фактичними матеріалами) і вироблення рекомендацій з її модернізації (у т.ч. служби особистої охорони керівника, технічних систем безпеки й т.д.);

• консультування з усіх аспектів особистої й корпоративної безпеки;

• підвищення рівня професійної підготовки співробітників існуючої системи безпеки підприємства;

• вироблення рекомендацій і створення правил поведінки працівників підприємства при виникненні надзвичайної ситуації;

• рекомендації з підготовки й проведення спеціальних заходів, спрямованих на виявлення можливих каналів витоку інформації.

Проведення тренінгів і відпрацювання навчальних ситуацій у сфері забезпечення різних питань безпеки підприємства із працівниками підприємства й співробітниками служби безпеки.

Створення системи охорони об'єктів різної категорії складності, що включає - відпрацьовування найбільш раціональної, відповідно до вимог Замовника, схеми охорони об'єкта, організації пропускного режиму.

Етапи:

• комплексне дослідження діючого режиму охорони об'єкта, пропускного режиму, виявлення недоліків;

• вивчення технології роботи об'єктів, на яких потенційно можливі розкрадання;

• відпрацювання моделей охорони об'єкта (у т.ч. з використанням технічних заходів охорони), пропускного режиму, протидії розкраданням;

• підбір співробітників охорони, виходячи з вимог Замовника, з урахуванням специфіки охорони об'єкта;

• укладання договору про надання охоронних послуг.

Проведення заходів щодо створення системи забезпечення безпеки функціонування юридичної особи, що містить у собі:

1.Вивчення умов діяльності й функціонування юридичної особи, що дозволяє комплексно й реально оцінити ступінь його захищеності від можливого виникнення й розвитку несприятливих факторів, спрогнозувати їхній вплив на його діяльність, діяльність його посадових осіб.

2. Відпрацювання елементів концепції забезпечення безпеки юридичної особи.

3. Відпрацювання комплексу заходів з попередження, локалізації негативних факторів, які можуть вплинути на діяльність юридичної особи, його посадових осіб.

**Тема 7. Захист службою безпеки підприємства об’єктів інформації, інформаційних систем від технічних розвідок та інших засобів таємного отримання інформації**

План:

Вступ.

1. Група ПДТР (протидії технічній розвідці): завдання і особливості діяльності.

2.Комплектування структурного підрозділу безпеки інформації (групи ПДТР) штатними спеціалістами.

3.Група захисту інформації від несанкціонованого доступу: завдан¬ня діяльності.

4. Криптографічний захист інформації. Завдання і мета діяльності криптографічної групи

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

**Вступ.**

На сучасному етапі серед основних реальних та потенційних загроз національній безпеці України в інформаційній сфері є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

Серед загроз, які можуть призвести до розголошення інформації, за своїми небезпечними наслідками особливе місце займають несанкціонований доступ до інформації, яка обробляється та циркулює на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також витік інформації технічними каналами.

Саме з метою протидії зазначеним загрозам в Україні створена та функціонує система технічного захисту інформації, яка дозволяє вирішувати практично весь комплекс завдань з технічного захисту інформації на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах державних органів, підприємств, установ та організацій.

Система являє собою сукупність *організаційних структур*, поєднаних цілями і завданнями захисту інформації, *нормативно-правової* та *матеріально-технічної* *бази* і спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Функції органу державного управління у сфері технічного захисту інформації виконує Департамент спеціальних систем та захисту інформації Служби безпеки України, який реалізує державну політику, здійснює управління захистом інформації в інформаційно-телекомунікаційних системах та на об’єктах інформаційної діяльності, а також державний контроль за функціонуванням системи технічного захисту інформації.

На відомчому рівні в центральних органах виконавчої влади, інших державних органах, підпорядкованих ним підприємствах, установах та організаціях створюються або визначаються підрозділи, на які покладаються завдання із забезпечення технічного захисту інформації.

На сьогодні в країні створено відповідну нормативно-правову базу, яка визначає основні принципи технічного захисту інформації, норми та вимоги з технічного захисту інформації, порядок проведення робіт та здійснення контролю його ефективності (більшість актів, що стосуються питань технічного захисту інформації, розміщено у мережі Інтернет на офіційному сайті Департаменту).

Функціонування системи технічного захисту інформації здійснюється з урахуванням необхідності забезпечення гарантії відповідності рівня захищеності інформації вимогам нормативних документів. При цьому необхідну якість робіт з технічного захисту інформації можна забезпечити за умови залучення спеціалістів, які мають відповідну фахову підготовку та досвід роботи, при відповідному технічному оснащенні.

Нині загальна кількість нормативно-правових актів, що регламен­тують діяльність в сфері технічного захисту інформації в нашій держа­ві, складає близько 150 одиниць.

Основу державного регулювання суспільних відносин в сфері ТЗІ становить Конституція України. До спеціального законодавства, що врегульовує дану галузь, належать Закони України: «Про інформацію», «Про державну таємницю», «Про захист інформації в автоматизованих системах», «Про Національну систему конфіденційного зв’язку», «Про Концепцію Національної програми інформатизації», «Про науково- технічну інформацію» та інші. У тому числі у сфері правоохоронної ді­яльності — такі, що визначають компетенцію та функції окремих дер­жавних органів влади: Служби безпеки України, міліції, прокуратури тощо (закони України «Про Службу безпеки України», «Про міліцію» та інші). Деякі вимоги щодо технічного захисту окремих видів інфор­мації містяться у законодавстві України про оперативно-розшукову ді­яльність, про організаційно-правові основи боротьби з організованою злочинністю.

Державна політика України у сфері захисту інформації від її вито­ку технічними каналами знаходить відображення у системі підзакон- них нормативно-правових актів органів державної влади, що видають­ся останніми відповідно до їх компетенції, функцій, прав і обов’язків. Дану систему складають Укази та Розпорядження Президента України, нормативно-правові акти Кабінету Міністрів України, нормативні акти Служби безпеки України, інших міністерств і відомств.

Розвиток положень чинного законодавства знаходить відображення у конкретних нормативно-правових актах, таких як:

1. Укази Президента України: від 22.04.1998 «Про деякі заходи щодо захисту інтересів держави в інформаційній сфері»; від

22.05.1998 «Про Положення про порядок здійснення криптографіч­ного захисту інформації в Україні»; від 27.09.1999 «Про Положення про технічний захист інформації в Україні»; від 10.04.2000 «Про заходи щодо захисту інформаційних ресурсів держави»; від 06.10.2000 « Питання Департаменту спеціал ьнихтелекомунікаційних систем та захисту інформації Служби безпеки України».

2. Постанови Кабінету Міністрів України: від 26.06.1996 №677 «Про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації»; від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні»; від

04.02.1998 № 121 «Про затвердження переліку обов’язкових ета­пів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних»; від

27.11.1998 № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави».

3. Накази ДСТСЗІСБ України: від 09.06.1995 № 25 «Про нормативні документи»; від 30.11.1999 № 53 «Про затвердження Положен­ня про порядок розроблення, виготовлення та експлуатації засо­бів криптографічного захисту конфіденційної інформації»; від

22.12.1999 № 61 «Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації»; від

29.12.1999  №62 «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації»; від 23.02.2002 № 9 «Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб».

Крім того, на сьогодні в Україні чинними є ряд нормативних доку­ментів (НД), що унормовують технічний захист інформації.

Це державні стандарти (ДСТУ 3396.0-96 Захист інформації. Тех­нічний захист інформації. Основні положення; ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт; ДСТУ 3396.2-96 Захист інформації. Технічний захист інформації. Тер­міни та визначення) та галузеві стандарти (НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від не­санкціонованого доступу; НД ТЗІ 1.1-003-99 Термінологія в галузі за­хисту інформації в комп’ютерних системах від несанкціонованого до­ступу; НД ТЗІ 2.5-004-99 Критерії оцінювання 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; НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення тех­нічного завдання на створення комплексної системи захисту інформації в автоматизованій системі).

Відповідно відносини у сфері ТЗІ як опосередкований об’єкт, ре­гулюються також законодавством та підзаконними нормативно-право­вими актами про державний нагляд за додержанням стандартів, норм і правил та відповідальність за їх порушення; про стандартизацію і серти­фікацію тощо.

Щодо системи технічного захисту інформації МВС України, до за­значених актів слід додати цілий ряд відомчих наказів, розпоряджень та вказівок, що регламентують діяльність підрозділів ТЗІ органів вну­трішніх справ.

Таким чином, на даний момент створено значний масив норматив­но-правових актів із зазначеного питання.

Конституція України є основним джерелом права у галузі технічно­го захисту інформації.

Відповідно до Конституції:

• забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу (стаття 17);

• кожному гарантується таємниця листування, телефонних роз­мов, телеграфної та іншої кореспонденції (стаття 31);

• ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України (стаття 32);

• кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань (стаття 34);

• кожен має право володіти, користуватися і розпоряджатися сво­єю власністю, результатами своєї інтелектуальної, творчої діяль­ності (стаття 41).

До міжнародних договорів, учасницею яких є Україна, слід віднести угоди в інформаційній та сфері безпеки інформації (наприклад, Угоду між Україною та Європейським Співтовариством про наукове і техно­логічне співробітництво, ратифіковану Законом України №368-ІУ від 25.12.2002, Угоду між Кабінетом Міністрів України та Урядом Республі­ки Білорусь про співробітництво в галузі технічного захисту інформації, ратифіковану Законом України №1434-ІУ від 04.02.2004 та інші). При­чому, положення, закріплені в даних угодах мають знайти свій розвиток у відповідній законодавчій базі, так як зазвичай такі міжнародні догово­ри носять узагальнений характер і вимагають певної деталізації.

Закони України, акти Президента України та Кабінету Міністрів України видаються Верховною Радою України, Президентом та Кабіне­том Міністрів України відповідно до їх компетенції. У цих актах отриму­ють розвиток положення Конституції України, Концепції національної безпеки, Доктрини інформаційної безпеки та міжнародних договорів, учасницею яких є Україна. Основне їх призначення — чітке регулюван­ня відносин, що виникають у сфері технічного захисту інформації, за­кріплення концептуальних положень у даній галузі.

Серед актів Служби безпеки України слід окремо вказати на таку ка­тегорію нормативів, як накази Департаменту спеціальних телекомуніка­ційних систем та захисту інформації Служби безпеки України (ДСТСЗІ СБ України), які пройшли відповідну реєстрацію в Міністерстві юсти­ції України. Однією з функцій СБУ є координація діяльності у сфері охорони державної таємниці (у тому числі — видання вказівок з цих пи­тань), а безпосередньо ДСТСЗІ СБ України реалізує державну політику у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, забезпечує функціонування державної системи урядового зв’язку і видає відповідні накази з зазначених питань. Причому, рішення Департаменту, прийняті в межах його повноважень, є обов’язковими для виконання центральни­ми і місцевими органами виконавчої влади, підприємствами, установа­ми та організаціями й громадянами.

Стосовно стандартизації в галузі ТЗІ слід зазначити, що, крім дер­жавній: стандартів України, діяльність з технічного захисту інформа­ції також регламентується нормативними документами системи тех­нічного захисту інформації (НД ТЗІ), які не належать до нормативних документів із стандартизації, але є обов’язковими для виконання всіма центральними і місцевими органами державної виконавчої влади, Уря­дом Автономної Республіки Крим, органами місцевого самоврядування, військовими частинами всіх військових формувань, створених відповід­но до законодавства, підприємствами, установами й організаціями не­залежно від форм власності, діяльність яких пов’язана з технічним за­хистом інформації.

І нарешті, положення з технічного захисту, що не знайшли свого ві­дображення у актах вищого рівня, врегульовуються для окремих органі­зацій, установ та державних органів відповідними відомчими наказами, розпорядженнями та вказівками, що регламентують діяльність підроз­ділів технічного захисту інформації, а також допомагають вирішувати певні конкретні завдання з ТЗІ. їх ми відносимо до актів інших органів, що видаються ними в межах наданої компетенції.

**1.** **Організація і функції підрозділів технічного захисту інформації**

Інформаційна безпека є комплексом, в якому не можна виділити важливіші чи менш важливі складові. її не можна сприймати інакше, ніж комплекс.

*Загрози інформаційній безпеці* - чинник або сукупність чинників, що створюють небезпеку функціонуванню й розвитку інформаційного простору, інтересам особистості, суспільства, держави. Основним питанням початкового етапу впровадження системи безпеки є призначення відповідальних осіб за безпеку і розмежування сфер їх впливу. Системні програмісти та адміністратори відносять це завдання до компетенції загальної служби безпеки, тоді як остання вважає, що цим питанням мають займатися спеціалісти по комп'ютерах.

Вирішуючи питання розподілу відповідальності за безпеку комп'ютерної системи, слід ураховувати такі правила:

* ніхто, крім керівництва, не може прийняти основоположні рішення в галузі політики комп'ютерної безпеки;
* ніхто, крім спеціалістів, не зможе забезпечити правильне функціонування системи безпеки;
* ніяка зовнішня організація чи група спеціалістів життєво не зацікавлені в економічній ефективності заходів безпеки.

Організаційні заходи безпеки інформаційних систем прямо чи опосередковано пов'язані з адміністративним управлінням і належать до рішень і дій, які застосовує керівництво для створення таких умов експлуатації, які зведуть до мінімуму слабкість захисту. Адміністрація здійснює:

* заходи фізичного захисту комп'ютерних систем;
* регламентацію технологічних процесів;
* регламентацію роботи з конфіденційною інформацією;
* регламентацію процедур резервування;
* регламентацію внесення змін;
* регламентацію роботи персоналу й користувачів;
* підбір і підготовку персоналу;
* заходи контролю і спостереження.

До стратегічних рішень при створенні системи комп'ютерної безпеки потрібно віднести розроблення загальних вимог щодо класифікації даних, котрі зберігаються і опрацьовуються в системі.

*Технічний захист інформації* (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Технічний захист секретної інформації спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Консультативні послуги в галузі технічного захисту інформації - розроблення та надання рекомендацій щодо організації (створення) комплексу технічного захисту інформації об'єкта інформаційної діяльності або інформаційної системи на підставі матеріалів їх дослідження; надання методичної допомоги в розробленні нормативно-правових актів, нормативних документів системи ТЗІ, проектної і робочої документації при створенні засобів або комплексів технічного захисту інформації, проведення експертизи таких документів.

Технічний захист інформації є важливим чинником реалізації організаційно-правових та інженерно-технічних заходів з метою запобігання витоку інформації за рахунок несанкціонованого доступу до неї, несанкціонованим діям та впливам на інформацію, які призводять до її знищення, порушення цілісності або блокування, а також протидії технічним розвідкам.

Слід дотримуватися заходів захисту в усіх точках мережі, за будь-якої роботи суб'єктів з корпоративною інформацією.

Правову основу технічного захисту інформації в Україні становлять:

* Конституція України;
* закони України;
* міжнародні договори України;
* угоди, обов'язковість виконання яких введена Верховною Радою України;
* укази Президента України;
* постанови Кабінету Міністрів України;
* розпорядження адміністрації Державної служби спеціального зв'язку та захисту інформації України;
* інші нормативно-правові акти з питань технічного захисту інформації.

Правову основу створення і діяльності ПЗІ становлять:

* Закон України "Про державну таємницю";
* Закон України "Про захист інформації в автоматизованих системах";
* Положення про технічний захист інформації в Україні;
* Положення про забезпечення режиму секретності під час оброблення інформації, що становить державну таємницю, в автоматизованих системах;
* інші нормативно-правові акти з питань захисту інформації;
* державні і галузеві стандарти;
* розпорядчі та інші документи.

Підрозділ захисту інформації (ПЗІ) здійснює діяльність відповідно до "Плану захисту інформації", календарних, перспективних та інших планів робіт, затверджених керівництвом компанії. Проте виконання будь-яких завдань структурними підрозділами залежить від суб'єктів системи технічного захисту, якості їхньої підготовки, професіоналізму, матеріального забезпечення і чіткої взаємодії з іншими структурами компанії та органами контролю.

Під *суб'єктом* у цьому разі розуміють користувача системи, процес, комп'ютер або програмне забезпечення для оброблення інформації. Кожен інформаційний ресурс (комп'ютер користувача, сервер організації або мережеве устаткування) має бути захищений від усіх можливих загроз.

Державна політика у сфері технічного захисту інформації формується згідно із законодавством і реалізується Держспецзв'язком у взаємодії з іншими суб'єктами системи технічного захисту інформації.

Метою створення ПЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) на підприємстві та здійснення контролю за її функціонуванням. На ПЗІ покладається виконання робіт з:

* визначення вимог щодо захисту інформації в автоматизованій інформаційній системі підприємства (АІС);
* проектування;
* - розроблення і модернізації КСЗІ;
* експлуатації;
* обслуговування;
* підтримки працездатності КСЗІ;
* контролю за станом захищеності інформації в комп'ютерних системах (КС).

Для проведення окремих заходів захисту інформації в КС, що пов'язані з напрямом діяльності інших підрозділів компанії, наказом керівництва визначають перелік, строки виконання робіт та виконавців - підрозділи або конкретних осіб. У своїй роботі ПЗІ взаємодіє з підрозділами компанії (режимно-секретним відділом, службою безпеки, відділом ділової розвідки, службою охорони та ін.), а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби до виконання робіт можуть бути залучені зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

У будь-якому каналі зв'язку виникають перешкоди, що призводять до спотворення інформації, яка надходить для опрацювання. Для зменшення вірогідності помилок вживають заходів щодо поліпшення технічних характеристик каналів, використання різних видів модуляції, розширення пропускної спроможності та ін. При цьому також потрібно вживати заходів щодо захисту інформації від помилок або несанкціонованого доступу.

Доступ - це надання можливості використовувати інформацію, що зберігається в ЕОМ (системі).

Будь-яка інформація в машині або системі потребує певного захисту, під яким розуміють сукупність методів управління доступом виконуваних у системі програм до інформації, що зберігається в ній.

Захисту підлягає будь-яка документована інформація, неправомірне поводження з якою може завдати збитку її власникові, користувачеві чи іншій особі.

Режим захисту інформації встановлюють щодо:

* відомостей, віднесених до державної таємниці уповноваженими органами на підставі чинного законодавства;
* конфіденційної документованої інформації власника інформаційних ресурсів або уповноваженою особою на законних підставах;
* персональних даних.

Завданнями підрозділу захисту інформації є:

1. Забезпечення безпеки інформації структурних підрозділів та персоналу компанії в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах із зовнішніми вітчизняними та закордонними організаціями.

2. Дослідження технології опрацювання інформації з метою виявлення:

\* можливих каналів витоку та інших загроз для безпеки інформації;

\* формування моделі загроз; розроблення політики безпеки інформації;

\* вивчення заходів щодо її реалізації.

3. Організація та координація робіт, пов'язаних із захистом інформації в компанії, необхідність захисту якої визначається чинним законодавством.

4. Підтримка необхідного рівня захищеності інформації, ресурсів і технологій.

5. Розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими має бути забезпечений захист інформації в компанії.

6. Організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу КС.

7. Участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів КС з питань захисту інформації.

8. Формування у персоналу і користувачів компанії розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації.

9. Організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації компанії.

10. Проведення контрольних перевірок виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації компанії.

11. Забезпечення визначених політикою безпеки властивостей інформації під час створення та експлуатації КС.

12. Своєчасне виявлення та знешкодження загроз для ресурсів КС, причин і умов порушення її функціонування та розвитку.

13. Створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні КС.

14. Ефективне знешкодження загроз для ресурсів КС або запобігання їм шляхом проведення комплексу правових, морально-етичних, фізичних, організаційних, технічних та інших заходів гарантування безпеки.

15. Керування засобами захисту інформації, керування доступом користувачів до ресурсів КС, контроль за їхньою роботою з боку персоналу ПЗІ, оперативне сповіщення про спроби НСД до ресурсів КС підприємства.

16. Реєстрація, збирання, зберігання, опрацювання даних про всі події в системі, які стосуються безпеки інформації.

17. Створення умов для максимально можливого відшкодування та локалізації збитків, завданих несанкціонованими діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками.

18. Зменшення негативного впливу наслідків порушення безпеки на функціонування КС.

Просочування конфіденційної інформації - це її безконтрольний вихід за межі ІС або через коло осіб, яким вона була довірена за видом служби або стала відома в процесі роботи. Цей витік може бути наслідком:

* розголошування конфіденційної інформації;
* витоку інформації різними, переважно технічними каналами;
* несанкціонованого доступу до конфіденційної інформації різними способами.

Розголошування інформації, що призвело до ознайомлення з нею осіб, не допущених до цих відомостей, можна кваліфікувати як умисні або необережні дії посадових осіб і користувачів, яким ці відомості були довірені у зв'язку зі службовою потребою. Можливий безконтрольний витік конфіденційної інформації візуально-оптичним, акустичним, електромагнітним та іншими каналами.

*Несанкціонований доступ* - це протиправне навмисне оволодіння конфіденційною інформацією особою, яка не має права доступу до відомостей, що охороняються. Найпоширенішими напрямами несанкціонованого доступу до інформації є:

* перехоплення електронних випромінювань;
* примусове електромагнітне опромінювання (підсвічування) ліній зв'язку з метою отримання паразитної модуляції;
* застосування підслуховуючих пристроїв (жучків);
* дистанційне фотографування;
* перехоплення акустичних випромінювань і відновлення тексту принтера;
* зчитування залишкової інформації в пам'яті системи після виконання санкціонованих запитів;
* копіювання носіїв інформації з подоланням заходів захисту;
* маскування під зареєстрованого користувача;
* маскування під запити системи;
* використання програмних пасток;
* використання недоліків мов програмування і операційних систем;
* незаконне підключення до апаратури і ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ інформації;
* зловмисне виведення з ладу механізмів захисту;
* розшифровування спеціальними програмами зашифрованої інформації;
* інформаційні інфекції.

Перелічені напрями несанкціонованого доступу потребують значних технічних знань і відповідних апаратних або програмних розробок з боку зломлювача. Використовують, наприклад, технічні канали витоку - фізичні шляхи від джерела конфіденційної інформації до зловмисника, за допомогою яких можна отримати відомості, що охороняються. Причиною виникнення каналів витоку є конструктивна й технологічна недосконалість схематичних рішень або експлуатаційне спрацювання елементів. Все це дає змогу зломлювачу робити перетворювачі, що діють за певними фізичними принципами і мають властивий цим принципам канал передачі інформації - канал витоку.

Під час створення та експлуатації КСЗІ компанії підрозділ захисту інформації виконує такі функції:

1. Організація процесу керування КСЗІ.

2. Розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій.

3. Вжиття заходів у разі виявлення спроб НСД до ресурсів КС, порушення правил експлуатації засобів захисту інформації або інших дестабілізаційних факторів.

4. Забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід із ладу або порушення режимів функціонування.

5. Організація керування доступом до ресурсів КС - розподіл між користувачами необхідних реквізитів захисту інформації:

* паролів;
* привілеїв;
* ключів та ін.

6. Супроводження й активізація бази даних захисту інформації:

* матриці доступу;
* класифікаційні мітки об'єктів;
* ідентифікатори користувачів тощо.

7. Спостереження (реєстрація і аудит подій в КС, моніторинг подій тощо) за функціонуванням КСЗІ та їх компонентів.

8. Підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в КС, впровадження нових технологій захисту і модернізації КСЗІ.

9. Організація і проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій КС або КСЗІ.

10. Участь у роботах з модернізації КС:

* узгодженні пропозицій щодо введення до складу КС нових компонентів;
* нових функціональних завдань;
* режимів оброблення інформації, заміни засобів оброблення інформації тощо.

11. Забезпечення супроводження й активізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їх зберігання і тестування.

12. Проведення аналітичного оцінювання поточного стану безпеки інформації в КС:

* прогнозування виникнення нових загроз та їх врахування в моделі загроз;
* визначення необхідності її коригування;
* аналіз відповідності технології оброблення інформації;
* аналіз реалізованої політики безпеки поточної моделі загроз та ін.

13. Доведення власникам інформації технічних можливостей захисту інформації в КС і типові правила для персоналу і користувачів КС.

14. Негайне втручання в процес роботи КС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника.

15. Регулярне подання звітів керівництву компанії-власника (розпорядника) КС про виконання користувачами КС вимог захисту інформації.

16. Аналіз відомостей про технічні засоби захисту інформації нового покоління.

17. Обґрунтування пропозицій щодо придбання засобів для компанії.

18. Контроль за виконанням персоналом і користувачами КС вимог, норм, правил, інструкцій щодо захисту інформації відповідно до визначеної політики її безпеки.

19. Контроль забезпечення режиму секретності у разі оброблення в КС інформації, що становить державну таємницю.

20. Контроль забезпечення охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що піддягають захисту.

21. Розроблення і реалізація спільно з PCB компанії комплексних заходів безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співпраці з іноземними фірмами.

22. Розроблення і реалізація спільно з PCB компанії комплексних заходів безпеки інформації під час проведення нарад, переговорів тощо, здійснення їх технічного та інформаційного забезпечення.

Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Зазвичай користувачі мають мінімальний набір привілеїв, адміністратори - максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але здебільшого - в процесі керування системою захисту, зокрема у разі недбалого користування привілеями.

Чітке дотримання правил керування системою захисту, принципу мінімуму привілеїв дає змогу уникнути таких порушень.

**2.Криптографічний захист інформації. Завдання і мета діяльності криптографічної групи.**

*Криптографічний захист інформації* — вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Типи засобів криптографічного захисту інформації

Залежно від призначення встановлюються такі категорії засобів КЗІ:

* засоби шифрування інформації;
* засоби, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ;
* засоби захисту від нав’язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізовують алгоритми криптографічного перетворення інформації, у тому числі засоби імітозахисту та електронного цифрового;
* засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми (далі – засоби категорії “Р”).

*Засіб криптографічного захисту інформації* – програмний, апаратно-програмний, апаратний або інший засіб, призначений для криптографічного захисту інформації.

*Електронний підпис* — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувала.

*Електронний цифровий підпис* (ЕЦП) (англ. digital signature) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

*Особистий ключ* – унікальний ідентифікатор, що використовується для ідентифікації

*Відкритий ключ* – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб’єктам відносин у сфері використання електронного цифрового підпису.

*Підставлення (заміна)*

*Ключ* — це секретний параметр для окремого контексту під час передачі повідомлення. Ключі мають велику важливість, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків.

*Переставлення*

*Шифрування з симетричними ключами* — схема шифрування, у якій ключ шифрування, та ключ дешифрування збігаються, або один легко обчислюється з іншого та навпаки, на відміну від асиметричного, де ключ дешифрування важко обчислити.

*Асиметричне шифрування*. На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, не зважаючи на пов’язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим.

*Криптографічна система, або криптосистема* (рос. – криптосистема, англ. – cryptosystem) – це сукупність програмних, апаратних, програмно-апаратних засобів, а також криптографічних алгоритмів або криптографічних схем і ключових параметрів, об’єднаних в єдину систему з метою роз’язання конкретної задачі захисту інформації.

**Тема 8. Організаційні заходи комплексного забезпечення безпеки підприємства як суб’єкта підприємницької діяльності**

**План:**

Вступ

1. Група режиму як підрозділ служби безпеки, її функції.
2. Збереження режиму таємності на підприємстві.
3. Служба охорони, її функції. Основні категорії об’єктів, що охороняються.
4. Пожежна служба. Основні вимоги до пожежної безпеки і обов’язки у цьому зв’язку керівника підприємства. Обов’язки начальника пожежної служби.

**СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

1. Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

13.Господарський кодекс України // Голос України. – 2003. – 14 березня.

14.Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців : Закон України від 15 травня 2003 р. // ВВР України. – 2003. – № 31 – 32. – Ст..263.

15. Горевий В.І. Юридичні документи підприємства : практикум, навчальний посібник // В. І. Горевий, А. М. Куліш. – Суми : ВТД «Університетська книга», – 2009. – 360 с.

16. Матузова В. К. Науково-практичний коментар Господарського кодексу України / В. К. Матузова. – К. : Хрінком Інтер, 2004. – 688с.

17. Бондарчук Ю. В. Безпека бізнесу: Організаційно-правові основи : науково-практичний посібник / Ю. В. Бондарчук, А. І. Марущак. – К. : Видавничий дім «Скіф», 2008. – 372 с.

**1.Завдання служби безпеки щодо гарантування режиму і охорони**

Основним завданням служби безпеки із забезпечення режиму і охорони є організація і здійснення заходів щодо гарантування безпеки діяльності й захисту інформації всіма можливими за певних умов способами і засобами.

Основними завданнями організації режиму і охорони є:

* o запобігання проникненню в службові приміщення, в зони, що охороняються, і на територію об'єкта сторонніх осіб;
* o забезпечення порядку внесення (винесення), ввезення (вивезення) матеріальних цінностей і входу (виходу) працівників і клієнтів.

Усі приміщення фірми залежно від призначення і характеру здійснюваних у них актів, дій або операцій поділяють на кілька зон доступності (безпеки), які враховують ступінь важливості різних частин об'єкта з огляду на можливі збитки від кримінальних загроз. Зони безпеки облаштовують послідовно - від огорожі на території об'єкта до сховища цінностей та інформації, почергово створюючи ланцюг перешкод, які доведеться долати зловмисникові.



**2. Структура служби безпеки**

Для забезпечення надійної охорони матеріальних цінностей, конфіденційних документів та інформації, що містить відомості комерційного характеру, а також для своєчасного запобігання спробам несанкціонованого доступу до них встановлюють певний режим діяльності, дотримання якого є обов'язковим для всіх працівників, відвідувачів і клієнтів.

Керівники і працівники фірми, що забезпечують і здійснюють режим охорони, керуються у своїй діяльності відповідним законодавством, нормативними документами і певними рекомендаціями. Види зон режими ості фірми наведено в табл. 3.7.

**Діяльність служби безпеки з організації контрольно-пропускного режиму на підприємстві**

Контрольно-пропускний режим - комплекс організаційно-правових обмежень і правил пропуску через контрольно-пропускні пункти в окремі будівлі (приміщення) працівників об'єкта, відвідувачів, транспорту і матеріальних засобів. Це один із ключових моментів в організації системи безпеки на підприємстві. Отже, контрольно-пропускним режимом є комплекс організаційних заходів (адміністративно-обмежувальних), інженерно-технічних рішень і дій служби безпеки.

**Таблиця класифікацій зон режимності фірми**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Категорія**  **режиму**  **доступу** | **Назва** | **Функціональне призначення** | **Умови доступу працівників** | **Умови доступу відвідувачів** | **Наявність охорони** | **Наявність технічних засобів охорони** |
| 0 | Вільна | Зона вільних відвідувань | Вільний | Вільний | Ні | Ні |
| 1 | Спостережувана | Зона прийому відвідувачів | Вільний | Вільний | Обмежена | Засоби спостереження і запису |
| 2 | Реєстраційна | Зона службових приміщень і кабінетів працівників | Обмежений службовою необхідністю | Реєстрований, 3 разовими перепустками | У 8 окремих зонах | Засоби охорони і контролю |
| 3 | Режимна | Зона керівного  складу,  спеціальних  підрозділів  фінансових  служб | Суворо обмежений | Реєстрований, 3 разовими перепустками із супроводом | Посилена  багатозонна | Засоби охорони, контролю і спостереження |

Організація контрольно-пропускного режиму пов'язана з певною складністю. Справа в тому, що механізм здійснення контрольно-пропускного режиму ґрунтується на застосуванні "заборон" і "обмежень" стосовно суб'єктів, що перетинають межі об'єктів, які охороняються, для забезпечення інтересів підприємства. Такий механізм має бути бездоганним за відповідністю вимогам чинного законодавства.

Розглянемо основні напрями створення контрольно-пропускного режиму на підприємстві: методику визначення та оцінювання початкових даних; розроблення заходів і нормативних документів; устаткування контрольно-пропускних пунктів.

Контрольно-пропускний режим як частина системи безпеки має відповідати чинному законодавству, статуту підприємства так іншим нормативно-правовим актам, що регулюють діяльність підприємства.

Основними цілями створення контрольно-пропускного режиму є:

* o захист законних інтересів підприємства, підтримка порядку внутрішнього управління;
* o захист власності підприємства, її раціональне й ефективне використання;
* o зростання прибутків підприємства;
* o внутрішня і зовнішня стабільність підприємства;
* o захист комерційних таємниць і прав на інтелектуальну власність.

Контрольно-пропускний режим як частина системи безпеки дає змогу вирішити такі завдання:

* o забезпечення санкціонованого проходження працівників і відвідувачів, ввезення (вивезення) продукції і матеріальних цінностей, ритмічної роботи підприємства;
* o запобігання безконтрольному проникненню сторонніх осіб і транспортних засобів на території, що охороняються, і в окремі будівлі (приміщення);
* o своєчасне виявлення загроз інтересам підприємства, а також потенційно небезпечних умов, що сприяють виникненню матеріального і морального збитку підприємства;
* o створення надійних гарантій підтримки організаційної стабільності зовнішніх і внутрішніх зв'язків підприємства, відпрацювання механізму оперативного реагування на загрози й негативні тенденції;
* o припинення посягань на законні інтереси підприємства, використання юридичних, економічних, організаційних, соціально-психологічних, технічних та інших засобів для виявлення і послаблення джерел загроз безпеці підприємства.

**ВИСНОВКИ З ПИТАННЯ**

Отже, контрольно-пропускний режим можна визначити і як систему забезпечення нормативних, організаційних і матеріальних гарантій виявлення, запобігання і припинення посягань на законні права підприємства, його майно, інтелектуальну власність, виробничу дисципліну, технологічне лідерство, наукові досягнення і інформацію, що охороняється, і як сукупність організаційно-правових обмежень і правил, що встановлюють порядок пропуску через контрольно-пропускні пункти працівників об'єкта, відвідувачів, транспорту і матеріальних цінностей.

Нормативні гарантії полягають у тлумаченні й реалізації норм права, з'ясуванні меж їх дії, у формуванні належних правовідносин, визначенні та забезпеченні правомірної діяльності підрозділів і працівників фірми з приводу її безпеки, використання обмежувальних заходів, застосування санкцій до фізичних і юридичних осіб, що посягають на законні інтереси фірми.

Організаційні гарантії формуються у процесі розроблення, побудови й підтримання високої працездатності загальної організаційної структури управління процесом виявлення й усунення загроз діяльності фірми, використання ефективного механізму стимулювання її оптимального функціонування, відповідної підготовки персоналу.

Матеріальні гарантії формуються за рахунок виділення і використання фінансових, технічних, кадрових, інтелектуальних, інформаційних та інших ресурсів фірми, що забезпечують своєчасне виявлення, ослаблення й усунення джерел загрози, запобігання можливому збитку і його локалізацію, створення сприятливих умов для діяльності фірми. Ці гарантії наповнюють нормативні й організаційні заходи безпеки практичним змістом, створюють реальну основу розвитку культури безпеки фірми.

Основні заходи контрольно-пропускного пункту розробляє служба безпеки, а затверджує керівник фірми. До них додається інструкція про контрольно-пропускний режим. Відповідальність за організацію контрольно-пропускного режиму покладається на начальника служби безпеки, практичне здійснення контрольно-пропускного режиму - на охорону (чергових по КІШ, контролерів, охоронців), працівники якої мають знати встановлені на об'єкті правила контрольно-пропускного режиму, документи, що діють, стосовно порядку пропуску на об'єкт (з об'єкта) працівників і відвідувачів, ввезення (вивезення) товарно-матеріальних цінностей. Контрольно-пропускний режим може бути встановлений як по об'єкту загалом, так і в окремих корпусах, будівлях, відділах, сховищах та інших спеціальних приміщеннях.

Вимоги до контрольно-пропускного режиму слід обов'язково довести до кожного працівника об'єкта. Всі працівники об'єкта зобов'язані дотримуватися їх. У кожному випадку порушення контрольно-пропускного режиму необхідно проводити адміністративне розслідування.

Обов'язки охорони з контрольно-пропускного режиму визначаються в інструкції і в посадових обов'язках контролерів контрольно-пропускних пунктів.

Підготовка вихідних даних. Підприємництво і заборони (обмеження) є суперечливими за своєю природою. Розробник контрольно-пропускного режиму має знайти розумний баланс між необхідними обмеженнями та інтересами підприємства.

**3.Розроблення заходів і нормативних документів контрольно-пропускного режиму** Його починають із визначення вихідних даних. Оцінюючи ці дані, розробник визначає основні положення інструкції про контрольно-пропускний режим. Доцільно запропонувати таку послідовність визначення й оцінювання вихідних даних:

* 1. Організаційна структура підприємства, розміщення його окремих елементів і характер виробництва (діяльності) на них. З'ясування цих питань дає змогу вирішити такі практичні завдання:
  + - виділити об'єкти, майданчики, будівлі і приміщення, на яких потрібно організувати контрольно-пропускний режим;
  + o визначити характер контрольно-пропускних пунктів (КПП) для пропуску працівників і транспортних засобів.
* 2. Оцінювання добового обсягу потоків транспортних засобів, вантажів, матеріальних цінностей і людей (персоналу фірми та відвідувачів), що проходять через КПП і в окремі будівлі (приміщення). Тільки на основі оцінювання реального стану місць пропуску можна визначити пропускну спроможність чинних КПП і привести її у відповідність із завданнями основного виробництва на об'єкті. Така оцінка допоможе вибрати оптимальний варіант автоматизації і контролю проходу (проїзду) на території, що охороняються.
* 3. Виділення (за ступенем важливості) категорії об'єктів, транспортних засобів і вантажів, а також категорії осіб, що перетинають установлені межі. Для досягнення чіткості у визначеннях доцільно класифікувати приміщення і територію об'єкта залежно від умов доступу і ступеня захищеності.

Для чіткої організації пропускного режиму слід поділити об'єкти підприємства (будівлі, приміщення) на загальнодоступні, закриті та з обмеженим доступом. Визначення категорій режиму може дати чітку відповідь на запитання, які потрібно з'ясувати під час організації контрольно-пропускного режиму і розроблення вихідної документації з устаткування об'єкта технічними засобами охорони.

Закріплення за приміщенням конкретної категорії допомагає регламентувати і обґрунтувати:

* o умови доступу працівників підприємства і відвідувачів на об'єкт;
* o пропозиції адміністрації підприємства для вироблення оптимального варіанта порядку пропуску осіб, транспортних засобів і матеріальних цінностей на об'єкт;
* o наявність і вид фізичної охорони;
* o види використовуваних технічних засобів для забезпечення безпеки.

Розробка інструкції про пропускний режим. Практичне вирішення питань, пов'язаних з організацією пропускного режиму, викладається в "Інструкції про пропускний режим", яка визначає систему організаційно-правових охоронних заходів щодо встановлення дозвільного порядку (режиму) проходу (проїзду) на об'єкт (з об'єкта) і має такі розділи:

* 1. Загальні положення, де зазначено:
  + o нормативні документи, на підставі яких складалася інструкція;
  + o визначення контрольно-пропускного режиму і мета його введення;
  + o посадові особи, на яких покладається організація і практичне керівництво контрольно-пропускною системою;
  + o санкції до порушників контрольно-пропускного режиму;
  + o вимоги до устаткування різних приміщень.
* 2. Порядок пропуску працівників підприємства, осіб, що відряджаються, і відвідувачів через контрольно-пропускні пункти. Тут містяться рекомендації:
  + o перерахувати всі КПП, подати їх призначення, опис, розміщення і встановити їх єдину нумерацію;
  + o викласти вимоги до устаткування КПП;
  + o установити порядок проходження працівників і відвідувачів на територію об'єкта і визначити категорії приміщень;
  + o визначити права і основні обов'язки контролерів КПП;
  + o установити приміщення, де забороняється приймати відвідувачів і представників сторонніх організацій.
* 3. Порядок допуску на об'єкт транспортних засобів, вивезення продукції, документів і матеріальних цінностей. У цьому розділі йдеться про:
  + o порядок допуску на територію об'єкта (з об'єкта) автотранспорту, що належить об'єкту;
  + o порядок в'їзду і стоянки на території об'єкта транспорту, що належить працівникам на правах особистої власності;
  + o порядок пропуску автомашин сторонніх організацій, що прибули з вантажем на адресу об'єкта в робочий і неробочий час;
  + o порядок вивезення (ввезення) товарно-матеріальних цінностей;
  + o правила оформлення документів на вивезення (винесення) матеріальних цінностей з території об'єкта.
* 4. Види перепусток, порядок їх оформлення. У цьому розділі викладено:
  + o види перепусток, їх кількість і статус;
  + o опис перепусток;
  + o порядок оформлення і видачі перепусток;
  + o порядок заміни і перереєстрації перепусток;
  + o заходи у разі втрати перепустки працівником.
* 5. Обов'язки посадових осіб з підтримання контрольно-пропускного режиму.
* 6. Облік і звітність, порядок зберігання і друку перепусток. Залежно від структури підприємства і характеру його діяльності інструкція може містити й інші розділи.

При розробленні інструкції про контрольно-пропускний режим визначають види і групи перепусток, які діятимуть на підприємстві. На великих підприємствах зазвичай установлюють кілька видів перепусток: постійні, тимчасові,разові й матеріальні. Зразки бланків перепусток розробляє адміністрація об'єкта (служба безпеки). За зовнішнім виглядом і змістом перепустки мають відрізнятися одна від одної і мати певні види захисту. Всі види перепусток, за винятком матеріальних, оформляє і видає бюро перепусток (або інший підрозділ) за письмовими заявками. Види перепусток визначають залежно від специфіки підприємства (рис. 3.3,3.4).

Постійні перепустки видаються співробітникам об'єкта, яких прийнято на постійну роботу, а також працівникам інших організацій, які постійно обслуговують об'єкт.



**Види пропускних документів на підприємствах**

Постійні перепустки можуть поділятися на групи, кількість і призначення яких визначаються інструкцією про контрольно-пропускний режим. Вони можуть зберігатися у працівників об'єкта або в кабінах на КПП. Постійні перепустки осіб, що вибувають з об'єкта на тривалий час (відпустка, хвороба, відрядження тощо), зберігаються в бюро перепусток (відділі персоналу), а у разі зберігання їх у кабіні КПП роблять відповідну відмітку. При звільненні працівника з роботи його перепустку показують в установленому порядку.

Тимчасові перепустки видаються особам, що працюють за контрактом, тимчасово прибули у відрядження на підприємства, і зберігаються зазвичай на КПП. Термін дії і порядок оформлення тимчасових перепусток визначаються інструкцією про контрольно-пропускний режим. Тимчасові перепустки можуть бути з фотографією і без неї; Без фотографи вони дійсні тільки у разі пред'явлення документа, що засвідчує особу.



**Види перепусток**

Разові перепустки (для відвідувачів і клієнтів) видаються на одну особу і лише для разових відвідин підприємства та його підрозділів. Вони дійсні за наявності документа, що засвідчує особу. Разові перепустки потрібно періодично змінювати за кольором бланків та іншими ознаками.

Разова перепустка, видана водієві транспортного засобу, може бути одночасно і разовою перепусткою для транспорту. Вона є дійсною для входу на територію об'єкта або його підрозділу протягом певного часу.

Контроль за відвідувачами підприємства з разовою перепусткою здійснюють, роблячи відмітку на зворотному боці перепустки про час відвідин і завіряючи підписом особи, що прийняла відвідувача.

Разову перепустку вилучає на КПП контролер, коли відвідувач виходить з об'єкта і здає її в бюро перепусток. Про осіб, що не вийшли з об'єкта після закінчення терміну дії перепустки, контролер повідомляє начальникові караулу (черговому по КІШ) для вжиття заходів щодо з'ясування причин затримання. Прізвища осіб, що відвідали об'єкт за разовою перепусткою, записують у спеціальну книгу обліку.

Разові перепустки дійсні протягом 30 хв. від моменту їх видачі до проходу контрольно-пропускного посту (КПП) і протягом 15 хв. після відмітки про час виходу відвідувача. Відмітку про час виходу робить на зворотному боці разової перепустки керівник підрозділу, до якого прибув відвідувач.

Матеріальні перепустки для вивезення (винесення) товарно-матеріальних цінностей видає адміністрація підприємства. Термін дії перепустки визначається інструкцією про контрольно-пропускний режим. Матеріальні перепустки вилучають на КПП і здають у бюро перепусток. їх видають на внесення (винесення) або ввезення (вивезення) матеріальних цінностей. За термінами дії вони прирівнюються до разових перепусток.

Зразки чинних перепусток мають бути на КПП.

**4.Устаткування пропускних пунктів**

Для дотримання пропускного режиму на підприємстві обладную контрольно-пропускні пункти. їх устаткування має забезпечувати необхідну пропускну спроможність і можливість ретельно перевіряти перепустку і документи осіб, що проходять, оглядати всі види транспорту, вантажі, що провозяться. Зокрема, вони повинні:

* o запобігати можливості несанкціонованого проникнення через КПП на об'єкт (з об'єкта) людей і транспортних засобів;
* o сприяти скороченню часу на перевірку документів, огляд транспорту і матеріальних цінностей;
* o уникати (зводити до мінімуму) помилок охоронця під час пропуску людей і транспорту;
* o дотримувати заходів безпеки охоронця під час огляду транспортних засобів.

Усі види КПП мають бути обладнані необхідними видами зв'язку і сигналізації для виклику резерву охорони. На КПП мають бути внутрішній телефон і список телефонів адміністрації підприємства.

Для підвищення ефективності служби пропускного режиму нині широко застосовують технічні засоби системи обмеження і контролю доступу. Грамотне використання цих систем дає змогу надійно забезпечити захист від несанкціонованого доступу не тільки на територію фірми, а й у приміщення і на об'єкти обчислювальної техніки, тобто на об'єкти, де обробляється конфіденційна інформація. Як видно з рис. 3.5, основними елементами системи є: зчитувач, контролер, виконавчий пристрій.

Щодо складніших систем застосовують системи централізованого управління. Вони складаються із комп'ютера (може бути система комп'ютерів, об'єднаних у локальну мережу) з широким програмним забезпеченням.

Зчитувач - це пристрій (розміщений у дверях або поряд з дверима), призначений для зчитування спеціальної кодової інформації, записаної на ідентифікаторі, й передачі цієї інформації у вигляді певного сигналу в контролер.



**Структурна схема системи обмеження і контролю доступу**

Контролер призначений для приймання та аналізу інформації, переданої зчитувачем, порівняння цієї інформації з еталонною, ухвалення на цій основі рішення про допуск відвідувача і видачі сигналу управління на виконавчий пристрій та в систему централізованого управління (за її наявності).

Виконавчими пристроями можуть бути електромеханічні (електромагнітні) замки, а також пристрої керування хвіртками, коморами, турнікетами тощо.

Для того щоб відвідувач потрапив на об'єкт (у приміщення), він має пред'явити зчитувачеві свій ідентифікатор - пристрій, на який записується кодова інформація, що однозначно ідентифікує його власника (рис. 3.6).

Електронні ключі "Touch Memory" є мікросхемою, розміщеною в міцному металевому корпусі. Кодова інформація записується в пам'ять цієї схеми. Код з електронного ключа прочитується при його торканні до зчитувача.

Картка із штриховим кодом - це пластина з нанесеними на неї смугами чорного кольору (штрихами). Кодова інформація міститься в ширині штрихів, що змінюється, і відстані між ними. Код з такої картки прочитується оптичним зчитувачем. На магнітну картку кодова інформація записується на магнітній смужці.

Перфорована картка є пластмасовою або металевою пластиною. Кодова інформація наноситься на неї у вигляді отворів, розміщених у певному порядку. Код з карток прочитується механічним або оптичним зчитувачем.



**Класифікація ідентифікаторів**

Кодова інформація на віганд-картці - це певним чином розміщена тонка металева смужка, приклеєна на картці спеціальним клеєм. Інформація з картки прочитується електромагнітним зчитувачем.

Безконтактна картка (Proximity) зберігає кодову інформацію в мікросхемі. Кодова інформація з безконтактних карток прочитується радіочастотним зчитувачем.

Останнім часом часто використовують так звані біометричні ідентифікатори. Хоча ставлення до них фахівців неоднозначне. Як ідентифікаційні ознаки можуть бути використані:

* o візерунок долоні;
* o голос людини;
* o відбиток пальця;
* o райдужна оболонка ока;
* o маса людини та ін.

Особливе місце серед ідентифікаторів посідають PIN-коди. Носієм кодової інформації є пам'ять людини. Працівник набирає на клавіатурі код і таким чином керує виконавчим пристроєм (наприклад замком дверей).

Використовуючи на практиці О і КД, можна з великою ефективністю забезпечити пропускний режим як на території фірми, так і в її окремому приміщенні, а отже, надійно вирішити проблему захисту від несанкціонованого доступу зловмисників в службові приміщення фірми, а також проблему несанкціонованого винесення (вивезення) матеріальних цінностей фірми.

Крім того, О і КД дасть змогу ефективно вирішувати завдання захисту конфіденційної інформації, що обробляється в деяких приміщеннях фірми. Це не тільки підвищить безпеку фірми як об'єкта, а й безпеку відомостей, що є комерційною таємницею фірми, а це, у свою чергу, знизить загальні витрати на гарантування безпеки фірми.

**Контрольно-пропускні пункти (КПП)**

Для проходження людей. На кожному КПП має бути кімната для охоронців, кімната для огляду громадян, камера схову, гардероб, турнікет з фіксувальними пристроями-замками. Розміщення приміщень визначено проектами і залежить від засобів механізації, автоматизації КПП та особливостей підприємства.

У контрольно-пропускному залі влаштовують проходи, обладнані технічними засобами охорони і фізичними бар'єрами. У комплекті устаткування, як правило є:

* o засоби механізації, автоматизації системи контролю доступу;
* o фізичні бар'єри (огорожі, турнікети, хвіртки);
* o основне і резервне освітлення;
* o засоби зв'язку і сигналізації;
* o системи відеоконтролю.

Як засоби контролю доступу можуть бути використані різні турнікети. Вони призначені для керування потоками людей і регулювання їх входу (виходу). Останнім часом найбільшого поширення набули електромеханічні турнікети. На відміну від громіздких і незручних механічних, ними легко керувати з пульта охоронця, вони можуть працювати у складі автоматизованої системи контролю доступу.

Вибираючи турнікети, потрібно зважати на те, що вони бувають "нормально відкриті" і "нормально закриті". "Нормально відкриті" турнікети (наприклад, розсувні, які донедавна були встановлені в російському метро) у світовій практиці використовують зрідка. Вони можуть вдарити людину, що проходить, і не дають змоги здійснювати ефективний контроль.

Для здійснення надійного контролю використовують здебільшого "нормально закриті" турнікети: роторні турнікети-вертушки, турнікети-тріподи і хвіртки.

Роторні турнікети-вертушки застосовують у випадках, коли потрібно повністю перекрити зону проходу. Вони можуть бути різними за висотою - від поясних до турнікетів на повний зріст, які конструктивно подібні до дверей, що обертаються.

Турнікети-тріподи з трьома планками, що перегороджують вхід, є одним із найбільш оптимальних засобів для здійснення контролю санкціонованого проходження. Вони мають сучасний вигляд, легко вмонтовуються, дають змогу здійснювати ефективний контроль доступу, оскільки розділяють потік людей поодинці, забезпечуючи при цьому високу пропускну спроможність. Триподи можна застосовувати в прохідних електронних системах, зокрема за великого потоку людей. Для запобігання можливості підлізти під планки турнікета або перестрибнути через них на турніку рекомендується встановлювати спеціальні датчики, які спрацьовують у разі спроби несанкціонованого проходу.

Хвіртки застосовують для керування потоками людей, організації вільного проходу в один бік (на вхід або вихід) і заборони проходу в інший. Хвіртки широко використовують у магазинах, аеропортах, на вокзалах. Застосування хвірток для контролю доступу неефективне. Це пов'язано з тим, що хвіртки не розділяють потік людей, оскільки після відкриття хвіртки через неї можуть пройти кілька осіб. Хвіртки можна встановлювати для організації вільного виходу, тоді як контроль входу довіряють триподам або вертушкам.

**Транспортні КПП**

До складу транспортного КПП входить оглядовий майданчик і службові приміщення. Оглядовий майданчик призначений для розміщення автомобілів під час їх огляду. Його можна обладнати як на території підприємства, так і за її межами або на території, що безпосередньо прилягає до КПП. Оглядовий майданчик:

* o має достатню площу для розміщення транспорту, що обстежується, технічні засоби для забезпечення нормальних умов роботи охоронця;
* o запобігає можливості несанкціонованого проникнення на об'єкт (з об'єкта) людей і транспортних засобів;
* o забезпечує за встановленої інтенсивності руху у будь-який час доби і року огляд автомобільного транспорту і вантажів, що перевозяться;
* o ізольований від інших споруд, що не стосуються охорони об'єкта і устаткування КПП;
* o гарантує безпеку охоронця під час виконання ним своїх обов'язків.

Розміри оглядового майданчика залежать від габаритів транспорту і вантажів, що перевозяться: довжина - 10-12, ширина -5-6 м.

На території, відведеній для обладнання оглядового майданчика, проводять планування місцевості з таким розрахунком, щоб на ній не затримувалися дощові й талі води - їх поперечний ухил має становити не менш як 2° від місця перебування охоронця у напрямі її бічних сторін (перпендикулярно проїжджій частині). Поверхню оглядового майданчика покривають бетоном або асфальтом. На проїжджій частиш майданчика виділяють місце зупинки транспорту для огляду, обмежене двома лініями "СТОП", що зроблені білою фарбою.

Перед в'їздом на оглядовий майданчик із зовнішнього боку основних і допоміжних воріт (шлагбауму), не ближче за 3 м від них, так само наносять поперечну лінію і напис "СТОП". Для гарантування безпеки руху транспорту не менш ніж за 100 м від воріт праворуч або над дорогою встановлюють вказівний знак "Рух в один ряд", а за 50 м від воріт - знак обмеження швидкості до 5 км/год.

Транспортні КПП можуть мати світлофори, ваги для зважування автомобілів, оглядову яму або естакаду для огляду вантажів, механізовані пристрої для автоматичного відкриття і закриття воріт з фіксаторами.

Оглядові майданчики за периметром обладнують фізичними бар'єрами і рубежем сигналізації. Зазвичай роблять огорожу з металевої сітки або декоративних ґрат до 2,5 м заввишки. На майданчику обладнують основні й допоміжні механізовані ворота. Основні ворота встановлюють на лінії основної огорожі об'єкта, а допоміжні - на протилежному боці оглядового майданчика. Замість воріт можна встановити механізовані шлагбауми. На автомобільних КПП використовують ворота з обмеженням і без обмеження габаритів за висотою. За конструкцією вони можуть бути орними або розсувними (висувними). Орні ворота обладнані фіксаторами.

Для регулювання руху транспорту, що проходить через проїзди оглядових майданчиків КПП, можна застосовувати двосекційні світлофори з лінзами червоного і зеленого кольору. До складу електромеханічного устаткування КПП для автомобільного транспорту зазвичай належать:

* o електродвигуни, привід воріт;
* o вимикачі автоматичного вимкнення електродвигунів за повністю закритих і відкритих стулок воріт;
* o магнітні пускачі електродвигунів;
* o електроустаткування світлофорів;
* o кабельні, силові лінії.

Розподільний щит (щит керування) може бути встановлений у приміщенні КПП, а за відсутності будівлі КПП - у спеціальній металевій шафі безпосередньо на оглядовому майданчику.

**Допуск на територію підприємства працівників, відвідувачів, транспортних засобів**

Прохід працівників і відвідувачів на територію об'єкта, в окремі підрозділи і назад здійснюється через контрольно-пропускні пункти за встановленими на об'єкті перепустками - основними документами, що дають право на прохід.

У неробочий час, вихідні і святкові дні допуск працівників на об'єкт має бути обмеженим - за попередніми заявками (списками) від керівників підрозділів, що завізовані начальником служби безпеки, з пред'явленням постійної перепустки. На підприємствах зі змінним режимом роботи до перепустки можуть бути додані спеціальні вкладки змінності.

Чергові спеціальних служб об'єкта (електрики, сантехніки, працівники зв'язку та ін.), що працюють позмінно, допускаються на територію об'єкта в неробочий час, у вихідні і святкові дні за списками, що підписані начальниками відповідних служб і затверджені начальником служби безпеки.

Відповідно до чинного законодавства і рішення адміністрації окремі категорії осіб користуються правом проходу на об'єкт без перепустки за пред'явлення службового посвідчення. До них належать:

* o працівники прокуратури;
* o працівники поліції за територіальністю;
* o інспектори праці, котлонагляду, енергонагляду за територіальністю;
* o посадові особи і окремі категорії працівників санітарно-епідемічної служби органів охорона здоров'я, що здійснюють санітарний нагляд.

Категорії осіб, що мають право пройти на об'єкт без перепустки (за службовими посвідченнями), мають бути чітко зазначені в інструкції про контрольно-пропускний режим.

Для забезпечення пропускного режиму на території об'єкта і в його структурних підрозділах наказом директора підприємства затверджується перелік підрозділів (приміщень), що мають певні категорії. У цих приміщеннях установлюють спеціальний режим і підвищену відповідальність за його дотримання працівниками цих підрозділів. Допуск у ці приміщення можливий суворо за списком, що узгоджений із службою безпеки. Приймання відвідувачів сторонніх організацій І підприємств, як правило, максимально обмежується. У всіх приміщеннях таких підрозділів мають бути вивішені списки працівників, що мають допуск. Всі приміщення після закінчення робіт оглядають чергові по підрозділах і особи, відповідальні за їх протипожежний стан. Після закінчення робочого дня ці приміщення закривають на замок, опечатують і здають під охорону.

Представник охорони перевіряє сигналізацію у присутності працівників, що здають приміщення. Ключі від цих приміщень в опечатаних пеналах здають під розписку начальникові караулу.

Отримують ключі до приміщень, обладнаних охоронною сигналізацією, особи, що мають право доступу до цих приміщень з пред'явленням постійної перепустки. Списки осіб, що мають право відкривати (закривати) зазначені приміщення, із вказівкою номерів карток, якими опечатуються приміщення, і номерів службових телефонів, підписує начальник підрозділу, затверджує начальник служби безпеки.

Усіх осіб, що намагаються пройти через КПП без пред'явлення перепустки, за чужою або неправильно оформленою перепусткою, пронести на об'єкт (з об'єкта) заборонені предмети, затримують і передають працівникам служби безпеки підприємства. Про кожний факт затримання начальник караулу або черговий по об'єкту складає службову записку про порушення пропускного режиму.

Допуск на територію (з території) підприємства транспортних засобів, що належать підприємству, можливий за пред'явлення водієм особистої перепустки зі спеціальним шифром або транспортної перепустки і дорожнього листка. Вантажників і осіб, що супроводжують транспорт, пропускають через КПП на загальних підставах.

Усі транспортні засоби під час проїзду через КПП потрібно оглядати. В'їзд і стоянка на території підприємства транспорту, що належить його працівникам на правах особистої власності, можливі за спеціальними списками.

Автомашини сторонніх організацій, що прибули з вантажем на адресу підприємства в робочий час, допускаються на територію за службовими записками з оглядом на транспортному КПП.

Залізничний транспорт і бригади, що його обслуговують, пропускають на підприємство за перепустками встановленого зразка, за списками або іншими документами , що визначені інструкцією про пропускний режим.

Опломбовані вагони і контейнери пропускають через КПП після їх зовнішнього огляду, якщо відтиски пломб відповідають відтискам у супровідних документах або накладних. У разі невідповідності відтисків, виявлення проломів вагона (контейнера) або обриву пломби вагон (контейнер) розкривають і оглядають у присутності представників адміністрації і залізниці.

Вивезення (винесення) готової продукції та інших матеріальних цінностей з території об'єкта можливі за матеріальними перепустками встановленого зразка.

Усі документи на матеріальні цінності, що вивозяться (виносяться) з підприємства, реєструються в бюро перепусток у книзі обліку і передаються в бухгалтерію.

Документи на вивезення (винесення) матеріальних цінностей мають бути виписані тільки на ту кількість вантажу (місць, ваги тощо), яка може бути вивезена (винесена) одночасно, і дійсні тільки на дату, вказану в дозвільному документі.

Будівельні й деревні відходи, макулатуру, металобрухт, металеву стружку рекомендується вивозити з території підприємства як матеріальні цінності. Вивезення з території об'єкта різного сміття, землі і снігу можливе без оформлення документів, але з обов'язковою реєстрацією на транспортному КПП.

Отже, система контрольно-пропускного режиму нерозривно пов'язана з гарантуванням безпеки підприємства. Будь-яка система безпеки об'єкта від загроз, пов'язаних з діями людини, техногенних або природних сил повинна мати систему ідентифікації за принципом "свій - чужий" або за рівнем доступу для захисту як об'єкта від проникнення сторонніх осіб, так і людини від небезпечних чинників, якщо вони є на об'єкті.

Установлюючи і забезпечуючи порядок переміщення персоналу і відвідувачів на території підприємства, система контрольно-пропускного режиму вирішує питання не тільки безпеки підприємства, а й раціональної організації праці.

Організаційно-адміністративні заходи та інженерно-технічні рішення в системі контрольно-пропускного контролю не можуть здійснюватися без зв'язку з іншими елементами системи безпеки об'єкта і повинні в неї вписуватися. Саме тому системи контролю доступу є обов'язковою структурою інтегрованих систем безпеки.

Враховуючи роль і місце контрольно-пропускного режиму в системі безпеки, слід застосовувати комплексний підхід до розроблення заходів обмеження доступу.

Вирішуючи завдання протидії тій чи іншій загрозі, розглядають у сукупності всі елементи системи:

\* дії підрозділів охорони;

\* технічні рішення;

o організаційно-адміністративні заходи.

Застосування комплексного підходу на етапі розроблення системи контрольно-пропускного режиму дає змогу уникнути зайвих витрат часу і ресурсів при створенні інтегрованої системи безпеки підприємства.

Створення інтегрованої системи безпеки потребує значних витрат. Проте, якщо уважно оцінити всі негативні чинники впливу на діяльність підприємства, ці витрати не здаються такими великими, оскільки забезпечують стійкий економічний розвиток підприємства і зводять до мінімуму можливі втрати. До того ж, процес створення інтегрованої системи безпеки може бути розтягнутий у часі з урахуванням матеріальних можливостей підприємства та умов його діяльності на ринку.

СТАТТЯ 264. Особистий огляд та огляд речей. Особистий огляд може провадитись уповноваженими на те посадовими особами органів Служби безпеки України, внутрішніх справ, органів і установ виконання покарань та слідчих ізоляторів, Військової служби правопорядку у Збройних Силах України, воєнізованої охорони, цивільної авіації, митних установ і органів прикордонної служби, а у випадках, прямо передбачених законами України, також і інших органів.

Особистий огляд може провадитись уповноваженою на те особою однієї статі з оглядуваним і в присутності двох понятих тієї ж статі.

Огляд речей, ручної кладі, багажу, знарядь полювання і лову риби, добутої продукції, транспортних засобів та інших предметів здійснюється, як правило, у присутності особи, у власності (володінні) якої вони є. У невідкладних випадках зазначені речі, предмети може бути піддано оглядові з участю двох понятих під час відсутності власника (володільця).”

**ЗАГАЛЬНІ ПОЛОЖЕННЯ ПОЖЕЖНОЇ БЕЗПЕКИ**

1. Пожежна безпека повинна забезпечуватися шляхом проведення організаційних, технічних та інших заходів спрямованих на попередження пожеж, забезпечення безпеки людей, зниження можливих майнових втрат і зменшення негативних екологічних наслідків у разі їх виникнення, створення умов для швидкого виклику пожежних підрозділів та успішного гасіння пожеж.

2. На кожному підприємстві повинен бути встановлений відповідний протипожежний режим, у т.ч. визначені:

- можливість (місце) паління, застосування відкритого вогню, побутових нагрівальних приладів;

- порядок проведення тимчасових пожежонебезпечних робіт (у тому числі зварювальних);

- правила стоянки та проїзду транспортних засобів;

- порядок прибирання горючого пилу та відходів, зберігання промасленого спецодягу, очищення повітроводів вентиляційних систем від горючих відкладень;

- порядок відключення від мережі електрообладнання у разі пожежі;

- порядок проходження посадовими особами навчання й перевірки знань пожежної безпеки, а також проведення з працівниками протипожежних інструктажів;

- порядок організації, експлуатації і обслуговування наявних технічних засобів протипожежного захисту (вогнегасників, протипожежного водопроводу, установок протипожежної сигналізації тощо);

- порядок проведення планово-попереджувальних ремонтів та оглядів електроустановок, опалювального, вентиляційного, технологічного та іншого обладнання;

- дії працівників у разі виявлення пожежі;

- порядок збирання членів добровільної пожежної дружини та відповідальних посадових осіб у разі виникнення пожежі, виклику вночі, у вихідні і св"яткові дні.

**2. ВИМОГИ БЕЗПЕКИ**

1. Території підприємств повинні постійно утримуватися в чистоті та систематично очищатися від сміття, відходів виробництва, тари, опалого листя, котрі необхідно регулярно вивозити у спеціально відведені місця.

2. Дороги, проїзди й проходи до будівель, споруд, пожежних вододжерел, підступи до зовнішніх стаціонарних пожежних драбин, пожежного інвентарю, обладнання та засобів пожежогасіння мають бути завжди вільними, утримуватися справними, взимку очищеними від снігу. Забороняється довільно зменшувати нормовану ширину доріг та проїздів.

3. До всіх будівель і споруд підприємства має бути забезпечений вільний доступ. Протипожежні розриви між будинками, спорудами, відкритими майданчиками для зберігання матеріалів, устаткування тощо повинні відповідати вимогам будівельних норм. їх не дозволяється захаращувати, використовувати для складування матеріалів, устаткування, стоянок автотранспорту.

4. Забороняється паління на території та в приміщеннях об'єктів по зберіганню ЛЗР, ГР і горючих газів. На території об’єктів, де паління дозволяється, адміністрація зобов’язана визначити і обладнати спеціальні місця для цього, позначити їх знаком або написом, встановити урну або попільницю з негорючих матеріалів.

5. Спецодяг,працюючих з лаками, фарба та іншими ЛЗР та ГР повинен своєчасно підлягати пранню та ремонту, зберігатися в розвішаному вигляді в металевих шафах, встановлених в спеціально відведених для цієї мети приміщеннях.

6. Електроустановки (можливість їх застосування, монтаж, наладка та експлуатація) повинні відповідати вимогам чинних Правил улаштування електроустановок (ПУЕ), Правил технічної експлуатації електроустановок споживачів (ПТЕ), Правил техніки безпеки при експлуатації споживачів (ПТБ) та інших нормативних документів.

7. НЕ ДОЗВОЛЯЄТЬСЯ:

            - проходження повітряних ліній електропередач та зовнішніх електропроводок над горючими покрівлями, навісами, складами паливно-мастильних матеріалів;

            - прокладка електричних проводів і кабелів транзитом через складські приміщення, пожежонебезпечні та вибухові зони;

            - експлуатація кабелів і проводів з пошкодженою або такою, що в процесі експлуатації втратила захисні властивості ізоляцією;

            - залишення під напругою кабелів та проводів з неізольованими струмопровідними жилами;

            - застосування саморобних подовжувачів;

            - користування пошкодженими розетками, відгалужувальними та з’єднувальними коробками;

            - застосування в пожежонебезпечних зонах складських приміщень люмінесцентних світильників з відбивачами і розсіювачами, виготовленими з горючих матеріалів;

            - складування горючих матеріалів на відстані 1 м від електроустаткування та під електрощитами.

8. Все електрообладнання (корпуси ел. машин, трансформаторів,апаратів, світильників, розп����дільчих щитів, щитів управління, металеві корпуси пересувних та переносних електроприймачів тощо) підлягає зануленню або заземленню відповідно до вимог розділів ПУЕ.

**3. ВИМОГИ ДО УТРИМАННЯ ПОЖЕЖНОЇ ТЕХНІКИ.**

**ПЕРВИННІ ЗАСОБИ ПОЖЕЖОГАСІННЯ.**

1. Пожежні автомобілі, мотопомпи та причіпи, введені в експлуатацію, повинні бути у повній готовності до виїзду (застосування) по тривозі: бути справним, мати повний комплект придатного до застосування пожежно-технічного озброєння, заправлені пальним, мастильними матеріалами, забезпечені запасом вогнегасних речовин.

2. Будівлі, споруди, приміщена, технологічні установки повинні бути забезпечені первинними засобами пожежогасіння, вогнегасниками, ящиками з піском, бочками з водою, покривалами з теплоізоляційного негорючого полотна, грубововняної тканини повсті, пожежними відрами, совковими лопатами, пожежним інструментом (гаками, ломами, сокирами тощо), які використовуються для локалізації і ліквідації пожеж у їх початковій стадії розвитку.

3. Норми належності первинних засобів пожежогасіння повинні встановлюватись нормами технологічного проектування, галузевими правилами пожежної безпеки з урахуванням рекомендацій Правил пожежної безпеки України.

4. Для розміщення первинних засобів пожежогасіння повинні встановлюватись спеціальні пожежні щити (стенди). На пожежних щитах необхідно вказувати їх порядкові номери та номер телефону для виклику пожежної охорони.

5. Пожежні щити повинні забезпечувати:

            - захист вогнегасників від попадання прямих сонячних променів;

            - зручність та оперативність зняття закріплених на щиті комплектуючих виробів.

6. Вогнегасники слід встановлювати у легкодоступних та помітних місцях (коридорах, біля входів або виходів з приміщень тощо), а також у пожежонебезпечних місцях, де найбільш вірогідна поява пожежі.

7. Переносні вогнегасники повинні розміщуватися шляхом:

            - навішування на вертикальні конструкції на висоті не менше 1.5 м. від рівня підлоги до нижнього торця вогнегасника і на відстані від дверей достатній для їх повного відчинення.

            - встановлення з пожежні шафи поруч з пожежними кранами, у спеціальні тумби або на пожежні щити;

8. Вогнегасники допущені до зведення з експлуатацію повинні мати:

            - облікові номери за прийнятою на підприємстві системою нумерації;

            - пломби на пристроях ручного пуску;

            - бірки та маркувальні написи на корпусі, червоне сигнальне пофарбування згідно з державними стандартами.

9. Використані вогнегасники, а також з зірваними пломбами необхідно

негайно направляти на перезарядження або перевірку. Вогнегасники відправлені з об"єкта на перезарядження, повинні бути замінені зарядженими.



ІНСТРУКЦІЯ

По забезпеченню пожежної безпеки  офісу

**1. Загальні положення**

1.1. Дана інструкція встановлює основні положення пожежної безпеки для приміщень, визначає необхідні заходи щодо попередження виникненню пожеж, визначає необхідні дії щодо евакуації і є обов’язковою для виконання всіма працівниками.  
1.2. Всі працівники, а також посадові особи, відповідальні за експлуатацію приміщень, повинні бути ознайомлені та дотримуватись всіх вимог даної інструкції.  
1.3. Відповідальність за дотримання вимог цієї інструкції у структурних підрозділах покладається на начальників структурних підрозділів.   
1.4. Працівники, винні в порушенні даної інструкції, в залежності від характеру порушень та їх наслідків, несуть відповідальність у встановленому чинним законодавством України порядку.

**2. Забезпечення протипожежної безпеки**

2.1. Безпечне в пожежному відношенні перебування людей в приміщеннях та попередження виникненню пожеж ЗАБЕЗПЕЧУЄТЬСЯ:  
· суворим додержанням працівниками вимог правил пожежної безпеки;  
· постійним утриманням в належному порядку шляхів евакуації та наявних в будівлі засобів протипожежного захисту.  
· розробкою планів евакуації людей та майна з приміщень з описом розподілу обов’язків між працівниками по евакуації людей та із зазначенням інших дій на випадок виникнення пожежі.  
· постійним підтриманням в робочому стані засобів протипожежної сигналізації та засобів оповіщення.  
· проведенням спеціальних навчань щодо пожежної безпеки.  
· своєчасним виконання протипожежних заходів, запропонованих органами Державного пожежного нагляду.

**3. Основні вимоги пожежної безпеки.**

Для належного утримання приміщень Адміністрація забезпечує виконання наступних вимог.  
3.1. Вимоги до приміщень  
3.1.1. Сходи та коридори повинні бути обладнані аварійним освітленням. Двері, які ведуть з загальних коридорів на сходи або безпосередньо з будинку, повинні бути доступними для евакуації.  
3.1.2. В коридорах, на сходових площадках і на дверях, які ведуть до шляхів евакуації, або безпосередньо на вулицю, повинно бути нанесене символічне зображення знаку “ВИХІД” - відчинених дверей з силуетом людини, яка біжить і стрілки, що вказує рух людини до виходу.  
3.1.3. Сходові площадки, евакуаційні виходи, проходи, коридори і тамбури повинні постійно утримуватись вільними від будь-яких предметів, що можуть перешкоджати руху людей.  
3.1.4. Меблі та обладнання мають бути розміщені таким чином, щоб постійно був забезпечений вільний евакуаційний прохід до дверей приміщення (завширшки не менш ніж 1 м.)  
3.1.5. Розташовані в коридорах і на сходових площадках шафи з електрощитами повинні бути завжди зачинені.  
3.1.6. Горища та технічний поверх (підвал) повинні утримуватись в чистоті і порядку. Вікна горищ і технічн��г�� поверху повинні бути зас��лені і зачинені. Двері і люки горищ, технічних поверхів, підвалів, вентиляційних камер повинні бути протипожежними з межею вогнетривкості 0,75 години і утримуватись в закритому (зачиненому) стані.  
3.1.7. На горищах та на технічному поверсі (у підвалі) не допускається зберігання горючих матеріалів або предметів.  
3.1.8. В будинку ЗАБОРОНЯЄТЬСЯ:  
 · зберігати на сходових площадках і в коридорах, а також під сходами будь-які легкозаймисті матеріали і меблі;  
· проводити відігрівання водопровідних, каналізаційних труб і труб центрального опалення паяльними лампами або іншими способами з застосуванням відкритого вогню;  
· проводити електрозварювальні роботи без попередньої очистки місця зварки від горючих матеріалів і без забезпечення місця проведення зварювальних робіт первинними засобами ліквідації пожежі;  
· палити та користуватись відкритим вогнем у підвалах, на горищах та інших місцях зберігання горючих матеріалів;  
· влаштовувати склади горючих матеріалів, в приміщеннях підвалів, горищ та цокольних поверхів;  
· застосовувати легкозаймисті та горючі рідини для миття підлоги;  
· залишати без нагляду електрообладнання і електроприлади, що знаходяться під високою напругою;  
· проводити сушку горючих матеріалів на радіаторах та інших приладах опалення.  
3.2. Електроприлади, електромережі та освітлення.  
3.2.1. Все електроустаткування повинно відповідати вимогам “Правил безпечної експлуатації електроустановок споживачів”. При розміщенні електроустаткування в приміщеннях слід ураховувати ризик перевантаження електричної мережі внаслідок потенційної одночасної роботи відповідного електроустаткування.  
3.2.2. Створення та експлуатація тимчасових електромереж не допускається.  
3.2.3. Все електроустаткування повинно мати захист від струмів короткого замикання та інших відхилень від нормальних режимів, які можуть викликати пожежу і загорання.  
3.2.4. В коморах з наявністю матеріалів, що горять, електросвітильники повинні бути обладнані захисними скляними ковпаками.  
3.2.5. При експлуатації електромереж та електроприладів ЗАБОРОНЯЄТЬСЯ:  
· користуватись електропроводкою з пошкодженою ізоляцією, несправним електроустаткуванням;  
· застосовувати для захисту електромережі замість автоматичних запобіжників та каліброваних плавких вставок захист кустарного виготовлення (жучки, скрутки, з дроту);  
· користуватись електропрасками, електроплитками, електро чайниками, електрокамінами та ін. нагрівальними приладами в приміщеннях, окрім спеціально призначених приміщень;  
· Проводити самостійно демонтаж електромереж та електроустаткування;  
· Складувати біля електрощитів, розеток папір і легкозаймисті матеріали.  
3.3. Утримання засобів гасіння пожежі.  
3.3.1. Приміщення мають бути забезпеченими первинними засобами гасіння пожежі.  
3.3.2. Використання пожежної техніки і первинних засобів гасіння пожежі не за призначенням категорично забороняється.  
3.3.3. Крани внутрішнього пожежного водопроводу повинні бути обладнані рукавами і стволами, розміщеними в запломбованих шафах. Пожежні рукави повинні бути сухими, добре скатаними і прикріпленими до кранів. Використання їх на господарські потреби категорично забороняється.  
3.3.4. На дверцятах шаф пожежних кранів повинен бути чітко вказаний індекс літерами “ПК”, його номер і номер виклику пожежної допомоги.  
3.3.5. Вогнегасники повинні розташовуватись на висоті не більш як 1,5 м від рівня підлоги до нижнього торця і на відстані не менш як 1,2 м від краю дверей при їх відчиненні.  
3.3.6. Вогнегасники повинні встановлюватись так, щоб було видно інструктивний надпис на його корпусі.  
3.3.7. Зарядка і перезарядка вогнегасників повинна проводитись згідно з інструкцією по їх експлуатації.  
3.3.8. Працездатність протипожежної сигналізації та засобів оповіщення повинна періодично перевірятися, згідно технічних вимог.

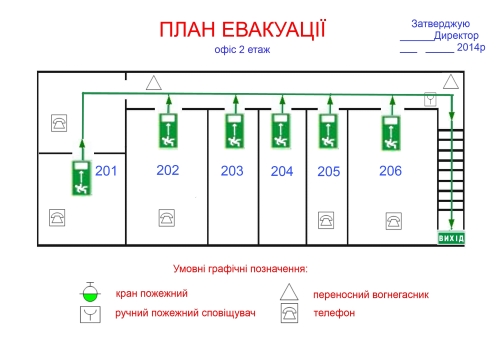
**4. Проведення необхідних навчань та контрольних заходів.**

4.1. Адміністрація забезпечує проведення первинних (при наймі на роботу) та щорічних навчань щодо пожежної безпеки та здійснює перевірки відповідності стану приміщень вимогам цієї інструкції.

**5. Попереджувальні заходи.**

Для забезпечення необхідного рівня пожежної безпеки працівники повинні:  
5.1. Пройти первинний та щорічний інструктаж щодо пожежної безпеки та вміти користуватися первинними засобами пожежогасіння та оповіщення та знати розташування запасних виходів.  
5.2. У разі виявлення пошкоджень електромереж та/ або електрообладнання негайно відключити прилади та повідомити працівників Адміністрації.  
5.3. Дотримуватися елементарних правил пожежної безпеки:  
5.3.1. Не палити в непередбачених для паління місцях та не кидати цигарки.  
5.3.2. Документи, папір та інші матеріали, що горять зберігати на відстані не менше 0,5 м. від світильників та 0,25 м. від приладів опалення.  
5.3.3. Після закінчення роботи  
· оглянути приміщення та переконатися у відсутності порушень, що можуть привести до пожежі;  
· відключити освітлення, електроживлення приладів та обладнання (за винятком обладнання, яке повинно працювати цілодобово).  
5.3.4. Електричні пристрої (ПК, копіювальні пристрої, тощо) мають бути встановлені тільки тими працівниками, які відповідають за забезпечення належної роботи цих пристроїв.

**6. У разі виявлення пожежі.**



6.1. При виникненні пожежі дії адміністрації в першу чергу спрямовуються на забезпечення безпеки та евакуації людей.  
6.2. При виникненні пожежі НЕОБХІДНО:  
· застосувати систему оповіщення;  
· негайно повідомити Адміністрацію;  
· негайно повідомити пожежну охорону по телефону (101), вказавши точну адресу і місце пожежі, що горить, наявність в будинку людей і своє прізвище;  
· до прибуття пожежної команди вжити заходів по евакуації людей і приступити до гасіння пожежі наявними засобами;  
· організувати евакуацію майна і матеріальних цінностей;  
· не користуватися ліфтом.  
 **Висновки з питання:**

При виникненні пожежі або загоранні керівники структурних підрозділів у приміщеннях, зайнятих цим структурним підрозділом, ЗОБОВ’ЯЗАНІ:  
· перевірити чи викликана пожежна допомога;  
· очолити керівництво гасінням пожежі до прибуття пожежних підрозділів;  
· під час пожежі необхідно утриматись від відчинення вікон і дверей, а також розбивати засклення.  
· евакуюючись з приміщення або будинку, потрібно зачинити за собою двері, так як притік свіжого повітря сприяє швидкому поширенню вогню.  
Після прибуття підрозділів пожежної охорони уповноважені особи, які керували гасінням пожежі, зобов’язані повідомити старшому начальнику пожежної охорони всі необхідні дані про наявність в будинку людей, про джерело пожежі, про заходи, вжиті по ліквідації пожежі.  
По кожному випадку пожежі або будь-якому загоранні Адміністрація досліджує всі обставини, що сприяли виникненню пожежі і загоранню і здійснює необхідні профілактичні заходи.

**ТЕМА 9. КАДРОВА СКЛАДОВА СОЦІАЛЬНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

**План.**

1.Кадрова безпека підприємства: об’єкти, види, індикатори.

2.Методи оцінки і збереження кадрової безпеки підприємства.

3.Захист конфіденційної інформації про особу.

4.Інформаційна безпека підприємства.

**Мета:** визначити сутність та основні завдання кадрової складової соціально-економічної безпеки підприємства; вивчити методи виявлення і збереження кадрової безпеки.

Вечканов, Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – СПб. : Питер, 2007. – 384 с.

2. Донець, Л. І. Економічна безпека підприємства : навч. посіб. для студентів вищих навч. закладів / Л. І. Донець, Н. В. Ващенко. – К. : Центр учб. літ., 2008. – 240 с.

3. Драган, О. І. Соціально-економічна безпека : конспект лекцій / О. І. Драган. – К. : Вища шк., 2013. – 114 с.

4. Економічна безпека : навч. посіб. / за ред. В. І. Франчука. – Львів : ЛьвДУВС, 2010. – 243 с.

5. Живко, З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. Л. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.

6. Захаров, О. І. Організація та управління економічною безпекою суб’єктів господарської діяльності : навч. посіб. / О. І. Захаров. – К. : КНТ, 2008. – 257 с.

7. Колот, А. М. Соціально-трудова сфера : стан відносин, нові виклики, тенденції розвитку : монографія / А. М. Колот. − К. : КНЕУ, 2010. − 251 с.

8. Крамаренко, Ю. М. Економічна безпека : навч. посіб. / Ю. М. Крамаренко, Є. О. Курта, О. В. Сировой. – Запоріжжя : ЛІПС, 2010. – 220 с.

9. Назарова, Г. В. Управління соціально-трудовою сферою підприємства : монографія / Г. В. Назарова, С. Ю. Гончарова, Н. В. Водницька ; за заг. ред. Г. В. Назарової. – Х. : ХНЕУ, 2010. − 323 с.

10. Отенко, І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : ХНЕУ, 2012. – 256 с.

11. Сергєєва, Л. Н. Соціально-економічна безпека : навч. посіб. / Л. Н. Сергєєва, Т. М. Книшенко, О. В. Лобань ; Класич. приват. ун-т. – Запоріжжя : Класичний приватний університет, 2011. − 107 с.

12. Соціально-економічна безпека : навч. посіб. / Г. О. Швиданенко [та ін.] ; за заг. та наук. ред. Г. О. ІІІвиданенко. − К. : КНЕУ, 2011. – 511 с

Належний рівень СЕБП залежить від складу кадрів, їхнього інтелекту та професіоналізму. Забезпечення кадрової складової СЕБП охоплює взаємопов’язані і водночас самостійні напрями діяльності, які спрямовані на роботу з персоналом. Кадрова складова СЕБП має на меті збереження стратегічно важливої ланки персоналу (топ менеджмент, працівників, що мають відношення до інтелектуальної власності, інноваційних розробок та конфіденційної інформації). З кадрами підприємства пов’язані основні внутрішні, а також зовнішні ризики, адже від економічних злочинів власних співробітників сьогодні страждають більше 40% компаній, втрачаючи в результаті крадок до 7% свого доходу, тільки 20% спроб злому мереж і отримання несанкціонованого доступу до комп’ютерної корпоративної інформації виникає ззовні, інші 80% випадків спровоковані за участю персоналу компанії. 95% збитків на підприємствах США утворюється за особистої участі персоналу підприємств і тільки 5 % – унаслідок дій клієнтів та інших осіб. Статистичні дані Європейського Союзу показують, що приблизно 58% відомих випадків шахрайства й зловживань припадає на частку службовців, 30% – менеджерів, а 12% – топ-менеджерів і власників. Кадрова безпека є поняттям складним і багатогранним, тому вітчизняні та зарубіжні автори виокремлюють різні підходи до його трактування. Кадрова безпека є уніфікованою категорією, яка виявляється на всіх рівнях управління від окремо взятого підприємства до системи національної економіки. Змістом категорії «кадрова безпека» є характеристика стану соціальноекономічної системи, при якому відбувається ефективне функціонування всіх її функціональних складових, забезпечення захищеності та здатність протистоянь внутрішнім і зовнішнім впливам і загрозам пов’язаних з персоналом, змістом. Кадрова безпека – це процес запобігання негативним впливам на економічну безпеку підприємства через ризики і загрози, пов’язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами.

До завдань кадрової безпеки належать: • забезпечення підприємства необхідними співробітниками, заповнення вакансій; утримання співробітників, їх розвиток; • розробка мотиваційних схем і схем оплати праці; • усунення збитку у зв’язку з трудовими суперечками; • підвищення лояльності співробітників; • аналіз кадрової ситуації у конкурентів; • робота із сайтами вакансій, кадровими агентствами; • аналіз ситуації на ринку праці в регіоні; • оцінювання підприємства як працедавця (погляд з боку співробітника); • заходи з проектування кар’єри (також погляд з боку співробітника). Кадрова безпека є комбінацією складових, пов’язаних між собою складними і часто завуальованими зв’язками: 1) Безпека життєдіяльності, яка включає: а) безпеку здоров’я (створення певних умов праці працівникам по запобіганню травматизму, захворювання на підприємстві); б) фізичну безпеку (виконання комплексу заходів, щодо недопущення порушень правил безпеки). 2) Соціально-мотиваційна безпека, яка включає: а) фінансову безпеку (грошово-кредитна платоспроможність працівників; впевненість в своєму робочому місці; оплата праці, яка враховує обсяг, кваліфікацію, професіоналізм і якість виконаної роботи); б) кар’єрну безпеку (професійно-кваліфікаційне та посадове просування працівників, заохочення в пристосуванні своєї кваліфікації до вимог робочого місця, в гарантіях виробничого зростання (планування кар’єри): підвищення особистої мобільності на ринку робочої сили; отримання шансів для самореалізації на робочому місці; в) естетичну безпеку (проведення загальноосвітніх семінарів, конференцій, групових дискусій; мотивація задоволення персоналу своєю роботою; поліпшення власного іміджу кожного працівника); г) адміністративно-незалежну безпеку (створення умов для відсутності можливості призначення непідготовлених і некомпетентних кадрів, що знаходяться у «родинних» стосунках з власниками, засновниками, акціонерами підприємства до керівництва трудового колективу персоналу). 3) Професійна безпека, яка включає: а) безпеку праці (система принципів, підходів, дій направлена на створення певних умов праці (рівень оплати праці, посада, обладнання робочого місця), з урахуванням новітнього, передового досвіду на ринку праці); б) інформаційну безпеку (прогнозування структури персоналу, визначення потреби в кадрах, планування, залучення та розміщення персоналу; оцінювання результатів праці для виявлення потенціалу кожного працівника); в) пенсійно-страхову безпеку (соціальний захист працівників (страхування, медичне обслуговування); г) інтелектуальну безпеку (безпека володіння знаннями, впровадження новітніх технологій у розвиток персоналу, удосконалення рівня професійних знань, умінь, здібностей у зв’язку з розвитком науково-технічного прогресу). 4) Антиконфліктна безпека, яка включає: а) патріотичну безпеку (створення психологічного клімату в колективі на основі позитивного відношення до підприємства, що характеризується психологічними показниками об’єднаності працівників, яка забезпечує узгодженість, безконфліктність спілкування, відповідальність та обов’язок, товариську допомогу, вимогливість до себе та іншого в інтересах виробництва); б) психолого-комунікаційну безпеку (сприяння міжособистісним комунікаціям і створенню сприятливого мікроклімату; врахування інтересів і побажань працівників, його особистого потенціалу; задоволеність міжособистісними стосунками по вертикалі (керівник-підлеглі) та горизонталі (виконавці)).

Аналізуючи структуру кадрової безпеки підприємства, доцільно виокремити інші пов’язані з нею ключові проблеми: ⎫ розроблення мотиваційних схем та схем оплати праці; ⎫ ліквідація збитків, пов’язаних з трудовими спорами; ⎫ аналіз ситуації конкурентів, аналіз ринку праці в регіоні; ⎫ робота з кадровим резервом, оцінка компанії як роботодавця; ⎫ способи проектування кар’єри; ⎫ підвищення лояльності та відповідальності співробітників тощо. При прийомі на роботу працівника роботодавець має зважати на низку важливих факторів. Серед них, зокрема, можна виділити наступні: • відповідність кваліфікації людини посаді, на яку вона претендує; • освіта за фахом; • особистісні якості людини. Серед методів підбору персоналу слід виділити розроблення та проведення тестів на виявлення професійної орієнтації, ерудиції, інтелекту, здібностей і розуміння, побудова професіограм. Якісна перевірка кандидатів під час прийому на роботу знижує ймовірність зловживань зі сторони персоналу. Серед зловживань в наш час найчастіше зустрічаються випадки підробки документів, фальсифікації витрат, пов’язаних з виконанням трудових обов’язків (відрядження, представницькі витрати), так звані «відкати» (один із найпоширеніших способів) популярні при несанкціонованих продажах і використаннях майна підприємства і т.п. Ефективність та продуктивність роботи персоналу залежить насамперед від таких, як: ¬ належні умови праці; ¬ можливість кар’єрного зростання; ¬ гідна винагорода; ¬ атмосфера у колективі; ¬ захист персональних даних та ін. 42 Кадрова безпека організації повинна будуватися на трудових та етичних відносинах інтелектуального потенціалу, які забезпечують стабільну і прибуткову роботу підприємства, запобігаючи як внутрішнім, так і зовнішнім загрозам, що сприяє розвиткові людського та соціального потенціалу, підвищенню рівня і якості життя населення.

**2 Методи оцінки і збереження кадрової безпеки**

Кадрова безпека відіграє домінуючу роль у системі безпеки підприємства, оскільки це робота з кадрами, а вони в будь-якій організації є головним ресурсом. Суб’єкти скоєння економічних злочинів, згідно з даними порталу Content Security, наявні у світі внутрішні та зовнішні загрози щодо кадрової безпеки розподіляються таким чином: - розголошення комерційної таємниці (зайва балакучість працівників) – 32%; - несанкціонований доступ до комерційної таємниці шляхом підкупу і схиляння до співпраці з боку конкурентів і злочинних угруповань – 24%; - відсутність у компанії належного нагляду і жорстких умов щодо забезпечення конфіденційності інформації – 14%; - традиційний обмін виробничим досвідом з працівниками інших компаній – 12%; 43 - безконтрольне використання інформаційних систем – 10 %; - наявність передумов виникнення серед персоналу конфліктних ситуацій, пов’язаних з відсутністю належної трудової дисципліни, психологічною несумісністю, випадковим підбором кадрів, слабкою роботою кадрів зі згуртування колективу – 8%. За даними дослідження Ernst & Young, рівень зафіксованого в Україні корпоративного шахрайства трохи вищий за середній у розвинених країнах (13%), але кращий за показники країн, що розвиваються (20%). Французька ж компанія Kroll Ontrack серед десяти основних тенденцій у сфері захисту інформаційних даних називає крадіжки за сприяння інсайдерів: сьогодні прогресивні організації роблять ставку на посилення безпеки за допомогою технологій, в той час як злочинці йдуть легшим шляхом – знаходять спільників серед персоналу. Окрім крадіжок інформації, можна зіштовхнутися і з чорним піаром з боку колишніх підлеглих, і з судовими позовами, що впливають на репутацію компанії, і з некомпетентністю «випадкового» працівника, і з помилками у кадрових документах. До найпоширеніших видів порушень при недотриманні кадрової безпеки належать: 1) афери з боку провідних спеціалістів (менеджерів і керівників середньої ланки, відповідальних за конкретний напрям бізнесу підприємства), в основному «за стінами» своєї фірми, зокрема у міжнародних організаціях; 2) фальсифікація сум «живих грошей» («готівки») у касі й сум на банківських рахунках, підробка чеків підприємства; 3) несанкціонований продаж і використання майна (власності) підприємства із корисливою метою; 4) оплата роботи підставних («фіктивних осіб»), так званих «пролісків»; 5) фальсифікація документації підприємства за допомогою електронної техніки й Інтернету (наприклад, перерахування коштів підприємства на свій особистий рахунок, внесення «потрібних» змін у звітні документи); 44 6) несанкціоновані операції із цінними паперами, матеріальними й нематеріальними активами підприємства; 7) фальсифікація звітів про використання коштів, виділених на відрядження, «представницькі видатки», на інші потреби підприємства. Мотивацію афер персоналу підприємства можна класифікувати так: • особисті фінансові труднощі, неможливість задоволення життєвих потреб своїх та сім’ї; • наявність слабких місць («дір») у системі управління діяльністю фірми (зокрема в системі бухгалтерського обігу); • низька кваліфікація керівництва підприємства; • нездоровий діловий клімат у колективі підприємства (наявність «скривджених»); • психологічна готовність (схильність) працівника до зловживання службовим становищем; • порочні зв’язки, вчинки, захоплення; • відсутність налагодженого контролю з боку керівництва за діяльністю персоналу; • слабкий кадровий менеджмент, що дає змогу займати відповідальні посади співробітникам-аферистам, неефективна персональна робота з кадрами. Забезпечення кадрової безпеки є найважливішою ланкою роботи менеджера (директора) із персоналу. Причому варто аналізувати як внутрішню, так і зовнішню небезпеку. Внутрішні фактори кадрової небезпеки такі: • невідповідність кваліфікації співробітників до займаної посади (небезпека, що спричиняє збитки); • недостатня кваліфікація працівників (проблема, вирішити яку зобов’язані кадровики); • слабка організація системи управління персоналом (немає філософії підприємства); 45 • слабка організація системи навчання (відсутня система обліку перспектив розвитку персоналу, що створює соціальну непевність у стабільності свого службового росту); • неефективна система мотивації (немає аналізу потреб кожної особистості й персональної мотивації); • помилки в плануванні ресурсів персоналу (найчастіше на просту роботу приймають висококваліфікований персонал); • відсутність творчого підходу до виконуваної роботи; • нецільове використання кваліфікованих співробітників; • орієнтація працівників на вирішення внутрішніх тактичних завдань; • відсутність орієнтації у співробітників на дотримання інтересів підрозділу (немає цільового управління); • відсутність або слабкість корпоративної політики; • неякісні перевірки кандидатів під час прийому на роботу. Зовнішні фактори кадрової небезпеки: ¬ кращі умови мотивації у конкурентів; ¬ установка конкурентів на переманювання найкращих працівників; ¬ зовнішній тиск на співробітників; ¬ втягування співробітників у різні види залежності; ¬ інфляційні процеси (їх слід ураховувати під час розрахунку заробітної плати). Ознаки правопорушення в поведінці співробітника і його неправомірні дії: 1) незвичне поводження працівника (нервозність, дратівливість, занепокоєння, перепади настрою, підозріла покірність тощо); 2) поява нестандартних даних і відхилення від звичайних (середніх) показників у бухгалтерських й/або інших документах; 3) зникнення окремих форм обліку та звітності (зокрема бланків) у бухгалтерській або іншій документації; 4) проведення сторонніх фінансових документів; 5) підробка підписів і виправлення даних у звітній документації; 46 6) надання ксерокопій документів замість оригіналів; 7) різке поліпшення матеріальних можливостей співробітника, не обґрунтоване його легальною діяльністю. Основні методи профілактики правопорушень персоналу: 1. Висококваліфікований кадровий менеджмент, використання сучасних технологій, персональна робота з кадрами й управління поведінкою персоналу. 2. Здійснення зовнішнього й внутрішнього аудиту діяльності керівних кадрів, розподіл їхніх функцій. 3. Періодичне відновлення повноважень (анулювання доручень, переділ функціональних обов’язків тощо). 4. Доручення комерційних справ не одному фахівцеві, а декільком - на конкурентній основі. 5. Розробка й дотримання сучасних методів охорони власності (майна) підприємства, зокрема коштів, інформаційних комунікацій. 6. Оптимізація системи фінансового обліку та звітності. 7. Обмеження доступу (допуску) співробітників до документів фінансової та бухгалтерської звітності. Для збереження кадрової безпеки варто використовувати сучасні кадрові технології, включаючи такі механізми: ефективну мотивацію; прискорену адаптацію (за рахунок наставництва); своєчасне запобігання конфліктним ситуаціям, атестацію; компенсацію; розумну політику звільнення; пропаганду корпоративності. Адаптація персоналу формується внаслідок психологічної сумісності з етичними цінностями компанії, соціальної сумісності в колективі, комфортності робочих місць, можливості задоволення своїх мотиваційних потреб, уваги керівництва тощо. Час адаптації – це не два місяці випробувального терміну, він індивідуальні для кожної особистості й кожної соціальної групи працівників.

**3.Зміст інформаційної безпеки. Поняття та класифікація загроз безпеки інформації та класифікація інформації з обмеженим доступом.**

Інформаційна безпека підприємства – це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства в цілісності, захист і гарантування повноти і точності інформації, яку вона видає, мінімізація руйнувань і модифікація інформації, якщо такі трапляються. Досягнення цієї мети потребує вирішення наступних задач: • віднесення інформації до категорії обмеженого доступу (службової таємниці); • прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів, визначення причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку; • створення умов функціонування з найменшою вірогідністю реалізації загроз безпеці інформаційних ресурсів; • створення механізму і умов оперативного реагування на загрози інформаційній безпеці з використанням правових, організаційних і технічних засобів забезпечення безпеки; • створення умов для максимально можливого відшкодування і локалізації збитку, що виникає внаслідок дії фізичних і юридичних осіб. Інформаційна безпека підприємства – це суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб’єкта господарської діяльності. Інформаційна безпека – це захищеність інформації та підтримуючої її інфраструктури від будьяких випадкових або зловмисних дій, результатом яких може з’явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури. Інформаційна безпека включає в себе заходи щодо захисту процесів створення даних, їх введення, обробки і виведення. 73 Інформаційна безпека – це комплекс заходів, які забезпечує для охоплюваної ним інформації наступні фактори: 1) конфіденційність – властивість, яка гарантує, що інформація недоступна і не може бути розкрита несанкціонованими особами, об’єктами чи процесами. Можливість ознайомитись з інформацією мають лише ті особи, які володіють відповідними повноваженнями; 2) цілісність – властивість, яка гарантує, що система повноцінно виконує свої функції без навмисних чи випадкових несанкціонованих втручань. Можливість внести зміни в інформацію повинні мати лише ті особи, які на це вповноважені; 3) доступність – можливість отримання авторизованого доступу до інформації з боку вповноважених осіб в відповідний санкціонований для роботи період часу. Облік ведеться засобами електронних реєстраційних журналів, які використовуються в основному лише вповноваженими службами. Забезпечення незмінності функціонування інформаційних систем має відбуватися на трьох рівнях: 1) адміністративному – за допомогою політики безпеки організації; 2) локальному – шляхом формування специфічних правил та рекомендаційних норм для персоналу; 3) об’єктному – використання сертифікованих, легальних засобів програмного та апаратного забезпечення. 5.2 Поняття та класифікація загроз безпеки інформації Сутність загроз щодо інформаційної безпеки зводиться до нанесення того чи іншого збитку підприємству (організації). Прояви можливого збитку можуть бути найрізноманітнішими: • моральна і матеріальна шкода діловій репутації організації; • моральний, фізичний чи матеріальний збиток, пов’язаний з розголошенням персональних даних окремих осіб; • матеріальний (фінансовий) збиток від розголошення конфіденційної інформації; 74 • матеріальний (фінансовий) збиток від необхідності відновлення порушених інформаційних ресурсів, які захищаються; • матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов’язань перед третьою стороною; • моральний і матеріальний збиток від дезорганізації в роботі всього підприємства. Джерела зовнішніх загроз можуть бути випадковими і запланованими та мати різний рівень кваліфікації. До них відносяться: - кримінальні структури; - потенційні злочинці і хакери; - нечесні партнери; - технічний персонал постачальників послуг, тощо. Внутрішні суб’єкти (джерела), як правило, представлені висококваліфікованими фахівцями у галузі розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв’язуваних завдань, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного устаткування і технічних засобів мережі. До них відносяться: - основний персонал (користувачі, програмісти, розробники); - представники служби захисту інформації; - допоміжний персонал (прибиральники, охорона); - технічний персонал. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути: а) зовнішніми: засоби зв’язку; мережі інженерних комунікації; транспорт; б) внутрішніми: неякісні технічні засоби обробки інформації; неякісні програмні засоби обробки інформації; допоміжні технічні засоби (охорони, сигналізації, телефонії); інші технічні засоби, що застосовуються в установі. Дії, які можуть завдати шкоди інформаційній безпеці підприємства, можна також розділити на 4 категорії: 75 1. Дії, які здійснюються авторизованими користувачами. У цю категорію потрапляють: цілеспрямована крадіжка або знищення даних на робочій станції або сервері; пошкодження даних користувачів у результаті необережних дій; 2. «Електронні» методи впливу, які здійснюються хакерами. До таких методів відносяться: несанкціоноване проникнення в комп’ютерні мережі, DOS атаки; 3. Комп’ютерні віруси. Окрема категорія електронних методів впливу – комп’ютерні віруси та інші шкідливі програми. Проникнення вірусу на вузли корпоративної мережі може призвести до порушення їх функціонування, втрат робочого часу, втрати даних, викраденні конфіденційної інформації і навіть прямим розкраданням фінансових коштів. Вірусна програма, яка проникла в корпоративну мережу, може надати зловмисникам частковий або повний контроль над діяльністю підприємства; 4. «Природні» загрози. На інформаційну безпеку підприємства можуть впливати різноманітні зовнішні фактори (неправильне зберігання, крадіжка комп’ютерів і носіїв, форс-мажорні обставини тощо). У сучасних умовах наявність розвиненої системи інформаційної безпеки стає однією з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якого підприємства (організації). Завдання забезпечення інформаційної безпеки повинно вирішуватися системно – різні засоби захисту (апаратні, програмні, фізичні, організаційні і т.д.) застосовуються одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз. Методи забезпечення інформаційної безпеки: • засоби ідентифікації і аутентифікації користувачів; • засоби шифрування інформації, що зберігається на комп’ютерах і що передається по мережах; • міжмережеві екрани; • віртуальні приватні мережі; 76 • засоби контентної фільтрації; • інструменти перевірки цілісності вмісту дисків; • засоби антивірусного захисту; • системи виявлення вразливостей мереж і аналізатори мережевих атак. Кожний з перерахованих засобів може використовуватись як самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційного захисту для систем будь-якої складності та конфігурації, незалежно від використовуваних платформ. «Комплекс 3А» включає аутентифікацію (або ідентифікацію), авторизацію і адміністрування. Ідентифікація та авторизація – це ключові елементи інформаційної безпеки. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій. Системи шифрування дозволяють мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересиланні по електронній пошті або передачу з мережних протоколів. Завдання даного засобу захисту – забезпечення конфіденційності. Основні вимоги, що пред’являються до систем шифрування, – високий рівень криптостійкості та легальність використання на території держави. Міжмережевий екран – це система або комбінація систем, що утворює між двома чи більше мережами захисний бар’єр, який захищає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних. Основний принцип дії міжмережевих екранів – перевірка кожного пакету даних на відповідність вхідної та вихідної IP-адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментації інформаційних мереж та контролю за циркулюванням даних. 77 Ефективний засіб захисту від втрати конфіденційної інформації – фільтрація вмісту вхідної і вихідної електронної пошти. Перевірка поштових повідомлень на основі правил, встановлених в організації, дозволяє також забезпечити безпеку компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму. Засоби контентної фільтрації дозволяють перевіряти файли всіх розповсюджених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється. Всі зміни на робочій станції або на сервері можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска. Це дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) таі ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум). Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об’єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися. Захист від вірусів може бути встановлено на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix-і Linuxсистеми, Novell) на процесорах різних типів. Фільтри спаму значно зменшують невиробничі витрати праці, пов’язані з розглядом спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ще не включені до бази антивірусних програм) часто мають ознаки спаму і фільтруються. Для протидії природним загрозам інформаційної безпеки в компанії має бути розроблений і реалізований набір процедур щодо запобігання надзвичай- 78 них ситуацій (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитків у тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних – резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій тощо. Основними принципами інформаційної безпеки підприємства є: ⎫ забезпечення цілісності і зберігання даних, тобто надійне їх зберігання в неспотвореному вигляді; ⎫ дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав); ⎫ доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації; ⎫ безперешкодний доступ до інформації в будь-який момент, коли вона може знадобитися підприємству. Ці принципи неможливо реалізувати без особливої інтегрованої системи інформаційної безпеки, що виконує наступні функції: - вироблення політики інформаційної безпеки; - аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачені або розсекречені дані); - планування заходів щодо забезпечення інформаційної безпеки; - планування дій в надзвичайних ситуаціях; - вибір технічних засобів забезпечення інформаційної безпеки. Етапи проведення робіт із забезпечення інформаційної безпеки підприємства: 1. Проведення обстеження підприємства на предмет виявлення реальних загроз несанкціонованого доступу до конфіденційної інформації. 2. Розробка політики безпеки, організаційно-розпорядчих документів і заходів щодо забезпечення інформаційної безпеки системи відповідно до вимог щодо захищеності технічних і програмних засобів від витоку конфіденційної інформації. 3. Проектування системи інформаційної безпеки. 79 4. Створення прототипу системи інформаційної безпеки. 5. Розробка зразка системи інформаційної безпеки. 6. Впровадження системи інформаційної безпеки в діючу структуру підприємства. 7. Навчання персоналу. 8. Атестація системи інформаційної безпеки підприємства. Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікація інформації, якщо такі трапляються. Для оцінки рівня інформаційної безпеки можуть бути використані коефіцієнти: - коефіцієнт повноти інформації (К пі) – розраховується як відношення обсягу інформації, що є в розпорядженні особи, яка приймає рішення (ОПР), і обсягу інформації, необхідної для ухвалення обґрунтованого рішення; - коефіцієнт точності інформації (К ті) – розраховується як відношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації; - коефіцієнт суперечливості інформації (К сі) – розраховується як відношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації. Обсяг інформації може бути розрахований у сторінках формату А4, кількості символів тексту, кількості авторських сторінок, Кбайтах, Мбайтах тощо. Рівень інформаційної безпеки (К і) може бути визначений на основі добутку трьох згаданих коефіцієнтів: К і = К пі × К ті × К сі , (5.1) При цьому, якщо: К і > 0,7 – рівень інформаційної безпеки високий; 0,3 > К і < 0,7 – рівень інформаційноїбезпеки середній; К і < 0,3 – рівень інформаційної безпеки низький. 80 В прагненні створення системи інформаційної безпеки і безпечного використання інформаційних технологій розроблено ряд міжнародних стандартів, методик та інших документів, що регламентують ці питання. Стандарти кібербезпеки (стандарти інформаційної безпеки) – це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити кібернетичне середовище користувача чи організації. Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж. Основна мета впровадження стандартів інформаційної безпеки – знизити ризики, включаючи попередження або пом'якшення кібер-атак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології. Стандарти кібербезпеки існували протягом кількох десятиліть, оскільки користувачі та постачальники співпрацювали на багатьох вітчизняних та міжнародних форумах для здійснення необхідних можливостей, політики та практики – як правило, вони з'являлися з роботи в Стенфордському консорціумі з досліджень з питань інформаційної безпеки та політики у 1990-х. Також багато завдань, які колись виконувалися вручну, зараз виконуються комп'ютером; тому існує потреба в забезпеченні інформації (ІА) та її безпеці. Американське дослідження 2016 року щодо затвердження рамок безпеки США повідомило, що 70 % опитаних організацій вважають NIST Cybersecurity Framework найбільш популярним передовим досвідом комп'ютерної безпеки, але багато хто відзначає, що для цього потрібні значні інвестиції. Головний службовець з питань інформаційної безпеки, як правило, покладається на вибір, впровадження та контроль ефективності стандартів кібербезпеки для організації. Види міжнародних стандартів кібербезпеки: ¬ BS 7799-1: 2005 — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні 81 правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом зі створення СУІБ, він визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризиків в контексті інформаційної безпеки. ¬ BS 7799-2: 2005 — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУІБ. Друга частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації. ¬ BS 7799-3: 2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт у сфері управління ризиками інформаційної безпеки. ¬ ISO/IEC 17799: 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005. ¬ ISO/IEC 27000 — Словник і визначення. ¬ ISO/IEC 27001 — «Інформаційні технології — Методи забезпечення безпеки — Системи управління інформаційної безпеки — Вимоги». Міжнародний стандарт, базувався на BS 7799-2: 2005. ¬ ISO/IEC 27002 — Зараз: ISO/IEC 17799: 2005. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». ¬ ISO/IEC 27005 — Зараз: BS 7799-3: 2006 — Керівництво з управління ризиками інформаційної безпеки. ¬ Німецьке агентство з інформаційної безпеки. Інструкція з захисту базової лінії — стандартні гарантії безпеки (керівництво по базовому рівню захисту інформаційних технологій). 82 У процесі впровадження міжнародних стандартів інформаційної безпеки створюється система менеджменту інформаційної безпеки підприємства, мета якої – скорочення матеріальних втрат, пов’язаних із порушенням інформаційної безпеки. Важливо, що ця система заощаджує підприємству кошти, а в деяких випадках захищає від банкрутства, і не є обов’язковою вимогою, що призводить до появи додаткової статті витрат. 5.3 Поняття та класифікація інформації з обмеженим доступом За умов жорсткої конкурентної боротьби захист ділової, фінансової, технологічної та іншої інформації від крадіжок, несанкціонованого використання, її зміни чи знищення набуває важливого значення. Інформація може бути відкритою або з обмеженим доступом. Конфіденційна інформація – це відомості, що перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значущою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право власника на її захист. Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законодовством таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Відомості, що належать до комерційної таємниці, мають містити такі ознаки: o не підпадають під державну таємницю; o стосуються виробничої діяльності фірми (підприємства); 83 o не спричиняють збитків інтересам суспільства; o мають дійсну або потенційну комерційну цінність і створюють переваги у конкурентній боротьбі; o мають обмеження у доступі, що встановлюються керівництвом фірми (підприємства); o щодо них на фірмі (підприємстві) вживаються заходи щодо їх охорони. До комерційної таємниці можуть бути віднесені: • технологія виробництва; • технологічні прийоми та устаткування; • модифікація раніше відомих технологій і процесів; • результати та програми наукових досліджень; • перспективні методи управління; • цінова і збутова політика; • порівняльні характеристики власного асортименту і товарів конкурентів з погляду якості, зовнішнього вигляду, пакування тощо; • виробничі, комерційні та фінансово-кредитні відносини з партнерами; • плани підприємства щодо розширення (скорочення) виробництва; • факти ведення переговорів з питань купівлі-продажу; • дані, що можуть бути використані для заподіяння шкоди репутації підприємства; • інформація про кадри підприємства; • наявність засобів та умов для захисту комерційної таємниці. Іноземні фірми в межах відомостей, які необхідно захищати за умов ринку, розглядають як промислову власність винаходи, дані про устаткування, інструменти, розроблені або придбані ними і недоступні для широкого користування. До промислових таємниць фірми відносять основні виробничі показники, проекти, технологічні інструкції, результати перевірок і випробувань, опис зразків продукції на сировину, сутність експериментів, оцінку якості процесів і виробів, дослідницькі звіти, карти контролю якості, інструкції з підготовки кадрів, вартісні показники, маркетингові дослідження, перелік покупців, умови постачань і стратегія на ринку, прогнози тощо. 84 Неправомірне збирання, розголошення та використання комерційної таємниці є видом недобросовісної конкуренції, який може становити досить серйозну загрозу економічній безпеці фірми (підприємства). Організація системи захисту інформації починається з визначення переліку відомостей, які є комерційною таємницею та конфіденційною інформацією. Керівник підприємства має затвердити наказом Положення про комерційну таємницю та про конфіденційну інформацію на підприємстві, в якому повинен бути наданий перелік таких відомостей і зазначити, що нерозголошення комерційної таємниці та конфіденційної інформації входить до трудових обов’язків працівників, та визначити відповідальність за невиконання цих обов’язків.

**4.Інформаційна безпека.**

Основна мета впровадження стандартів інформаційної безпеки – знизити ризики, включаючи попередження або пом'якшення кібер-атак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології. Стандарти кібербезпеки існували протягом кількох десятиліть, оскільки користувачі та постачальники співпрацювали на багатьох вітчизняних та міжнародних форумах для здійснення необхідних можливостей, політики та практики – як правило, вони з'являлися з роботи в Стенфордському консорціумі з досліджень з питань інформаційної безпеки та політики у 1990-х. Також багато завдань, які колись виконувалися вручну, зараз виконуються комп'ютером; тому існує потреба в забезпеченні інформації (ІА) та її безпеці. Американське дослідження 2016 року щодо затвердження рамок безпеки США повідомило, що 70 % опитаних організацій вважають NIST Cybersecurity Framework найбільш популярним передовим досвідом комп'ютерної безпеки, але багато хто відзначає, що для цього потрібні значні інвестиції. Головний службовець з питань інформаційної безпеки, як правило, покладається на вибір, впровадження та контроль ефективності стандартів кібербезпеки для організації. Види міжнародних стандартів кібербезпеки: ¬ BS 7799-1: 2005 — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні 81 правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом зі створення СУІБ, він визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризиків в контексті інформаційної безпеки. ¬ BS 7799-2: 2005 — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУІБ. Друга частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації. ¬ BS 7799-3: 2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт у сфері управління ризиками інформаційної безпеки. ¬ ISO/IEC 17799: 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005. ¬ ISO/IEC 27000 — Словник і визначення. ¬ ISO/IEC 27001 — «Інформаційні технології — Методи забезпечення безпеки — Системи управління інформаційної безпеки — Вимоги». Міжнародний стандарт, базувався на BS 7799-2: 2005. ¬ ISO/IEC 27002 — Зараз: ISO/IEC 17799: 2005. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». ¬ ISO/IEC 27005 — Зараз: BS 7799-3: 2006 — Керівництво з управління ризиками інформаційної безпеки. ¬ Німецьке агентство з інформаційної безпеки. Інструкція з захисту базової лінії — стандартні гарантії безпеки (керівництво по базовому рівню захисту інформаційних технологій). У процесі впровадження міжнародних стандартів інформаційної безпеки створюється система менеджменту інформаційної безпеки підприємства, мета якої – скорочення матеріальних втрат, пов’язаних із порушенням інформаційної безпеки. Важливо, що ця система заощаджує підприємству кошти, а в деяких випадках захищає від банкрутства, і не є обов’язковою вимогою, що призводить до появи додаткової статті витрат. 5.3 Поняття та класифікація інформації з обмеженим доступом За умов жорсткої конкурентної боротьби захист ділової, фінансової, технологічної та іншої інформації від крадіжок, несанкціонованого використання, її зміни чи знищення набуває важливого значення. Інформація може бути відкритою або з обмеженим доступом. Конфіденційна інформація – це відомості, що перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значущою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право власника на її захист. Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законодовством таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Відомості, що належать до комерційної таємниці, мають містити такі ознаки: 1. не підпадають під державну таємницю; 2. стосуються виробничої діяльності фірми (підприємства); 3. не спричиняють збитків інтересам суспільства; 4. мають дійсну або потенційну комерційну цінність і створюють переваги у конкурентній боротьбі; 5. мають обмеження у доступі, що встановлюються керівництвом фірми (підприємства); 6. щодо них на фірмі (підприємстві) вживаються заходи щодо їх охорони. До комерційної таємниці можуть бути віднесені: • технологія виробництва; • технологічні прийоми та устаткування; • модифікація раніше відомих технологій і процесів; • результати та програми наукових досліджень; • перспективні методи управління; • цінова і збутова політика; • порівняльні характеристики власного асортименту і товарів конкурентів з погляду якості, зовнішнього вигляду, пакування тощо; • виробничі, комерційні та фінансово-кредитні відносини з партнерами; • плани підприємства щодо розширення (скорочення) виробництва; • факти ведення переговорів з питань купівлі-продажу; • дані, що можуть бути використані для заподіяння шкоди репутації підприємства; • інформація про кадри підприємства; • наявність засобів та умов для захисту комерційної таємниці. Іноземні фірми в межах відомостей, які необхідно захищати за умов ринку, розглядають як промислову власність винаходи, дані про устаткування, інструменти, розроблені або придбані ними і недоступні для широкого користування. До промислових таємниць фірми відносять основні виробничі показники, проекти, технологічні інструкції, результати перевірок і випробувань, опис зразків продукції на сировину, сутність експериментів, оцінку якості процесів і виробів, дослідницькі звіти, карти контролю якості, інструкції з підготовки кадрів, вартісні показники, маркетингові дослідження, перелік покупців, умови постачань і стратегія на ринку, прогнози тощо. 84 Неправомірне збирання, розголошення та використання комерційної таємниці є видом недобросовісної конкуренції, який може становити досить серйозну загрозу економічній безпеці фірми (підприємства). Організація системи захисту інформації починається з визначення переліку відомостей, які є комерційною таємницею та конфіденційною інформацією. Керівник підприємства має затвердити наказом Положення про комерційну таємницю та про конфіденційну інформацію на підприємстві, в якому повинен бути наданий перелік таких відомостей і зазначити, що нерозголошення комерційної таємниці та конфіденційної інформації входить до трудових обов’язків працівників, та визначити відповідальність за невиконання цих обов’язків. Ключові категорії за темою