та обмеження доступу до секретних носіїв, перевірка персоналу, та встановлення відповідальності за порушення правил.

Технічні заходи вони слугують для закриття каналів витоку інформації.

До таких заходів належать використання спеціальної апаратури, яка буде, покращувати рівень безпеки, а також програмне забезпечування екранування та заземлення, звукоізолювання виділених приміщення, установлення засобів і систем для виявлення закладних пристроїв.

**Список використаних джерел:**

1. Про Національну програму інформатизації : Закон України № 74/98-ВР від 04.02.1998 [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/ document%5C1542964%5Czakon1.htm. – Назва з екрану.

2. Ильганаева В. А. Социальные коммуникации (теория, методология, деятельность) : словарь-справоч. / авт.-сост. В. А. Ильганаева. – Х. : КП «Городская типография», 2009. – 392 с.

3. Діловодство й архівна справа. Терміни та визначення понять: ДСТУ 2732:2004 / розроб.: О. Загорецька, Л. Драгомірова, Л. Кузнєцова, С. Кулешов та ін. – К. : Держспоживстандарт України, 2005. – 32 с.

4. Архівознавство : підруч. для студ. іст. ф-тів вищ. навч. закладів України / за заг. ред. Я. С. Калакури та І. Б. Матяш. – К. : Видавн. Дім«КМ Академія», 2002. – 356 с.

5. Наказ «Про затвердження Положення про умови зберігання архівних документів». 15.01.2003 / Державний комітет архівів України-п. 3; 4; 9.

**Кучмай Є.В., Власюк В.М.**
*студенти,*
*Навчально-науковий інститут інформаційної безпеки*
*Національної академії Служби безпеки України*

## СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

В залежності від можливих порушень в системі та різного виду несанкціонованого доступу до інформації існує велика кількість видів технологій сучасного захисту, що можливо розділити на окремі групи: морально – етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Необхідно відмітити, що такий поділ є досить умовним.

Морально-етичні технології. В цю групу входять норми поведінки в роботі з ЕОМ, в роботі з мережею. Такі норми не є обов’язковими до виконання та не закріплені на законодавчому рівні, але невиконання таких норм веде до зниження авторитету та престижу людини. Група морально-етичних норм можуть бути як неписаними, так можуть бути сформовані та закріплені в статуті.

До адміністративних технологій захисту інформації відносять процеси функціональності 1С, діяльність персоналу підприємства, порядок взаємодії користувачів інтернету із системою таким чином, щоб зменшити вплив на систему та не допустити порушень безпеки в роботі системи [5, с. 33].

Технології фізичного (технічного) захисту інформації – це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів 1С, стихійних лих, саботажу, диверсій і т. ін.

Основні технології захисту: оснащення приміщень генераторами шуму, виконання вимог безпеки в приміщенні, використання актуальних антивірусів.

За допомогою пристрою передачі можуть бути встановлені засоби для захисту інформації, розрізняють наступні типи:

– програмні (truecrypt, bitlocker);

– апаратні (datashur, samurai);

– програмно-апаратні (shipka, key_p1, rutoken) [3, с. 29].

Програмні засоби дозволяють здійснювати аутентифікацію користувачів на ПК, шифрувати інформацію. Існують апаратні рішення, які здійснюють автоматичне шифрування інформації на з'ємні носії після процедури аутентифікації. Програмно-апаратний комплекс пристроїв підвищує безпеку, але також вимагає аутентифікацію.

Аутентифікація – процедура перевірки автентичності входить в систему об'єкта, результатом зазвичай є авторизація, тобто надання суб'єкту певних прав доступу до ресурсів системи.

Процедура аутентифікації повинна бути максимально захищена, тому що витік даних для аутентифікації є дуже критичним для безпеки.

Існує досить багато методів аутентифікації:

– За допомогою PIN коду або пароля.

– За допомогою одноразових паролів.

– Біометрична, яка поділяється на велику кількість різних методів аутентифікації (відбиток пальця, геометрія особи, геометрія руки, райдужна оболонка ока, голос, малюнок вен, почерк і т. д.).

– За допомогою смарт-карти, USB ключа.

– За цифровому сертифікату [6, с. 44].

Роботи зі створення нових методів щодо забезпечення авторизації тривають і сьогодні, існують і різні екзотичні варіанти, які в майбутньому можуть знайти своє застосування. Наприклад, для проходження аутентифікації може знадобитися правильно розставити фігури на шаховому полі відповідно до заданої комбінації або ввести своє число з великої кількості чисел (наприклад, число формується першою і останньою цифрою).

На етапі передачі інформації по оптоволоконній лінії, на з'ємних носіях, по радіоканалу або іншими способами інформація може бути модифікована, отримана третіми особами або пошкоджена [2, с. 39].

Способи захисту: шифрування переданої інформації, екранування ліній передачі інформації, додавання елементів контролю переданих даних.

На етапі прийому інформації пристроєм другого користувача може виявитися, що відправлена першим користувачем інформація була змінена або модифікована, а також пошкоджена.

Способи захисту: передана інформація повинна бути зашифрована, для контролю отриманих даних і перевірки їх приналежності відправнику повинна бути використаний електронно-цифровий підпис файлів, який дозволить не тільки провести ідентифікацію відправника, а й перевірити цілісність документа [1, с. 66].

Захист від шпигунських пристроїв. Ні для кого, ні секрет, що в інтернеті можна недорого купити пристрій у вигляді флешки, яка зможе непомітно для користувача зіграти в операційній системі роль клавіатури і мишки і виконати поставлений сценарій (скопіювати інформацію на накопичувач, відкрити віддалений доступ до комп'ютера жертви і ін. ). Пристрій Key_P1, розроблений компанією Мультіклет дозволяє заблокувати дану шкідливу апаратуру, виконавши так звану функцію апаратного фільтра між ПК і накопичувачем.

Шифрування на накопичувачах інформації здійснюється за секторами. Для шифрування на накопичувачах застосовується 1 024 ключів, тобто один файл в залежності від розміру може бути зашифрований декількома сотнями ключів [5, с. 48].

Шифрування інформації, як на ПК, так і на накопичувачах може здійснюватися за допомогою синхронних ключів. Це ключі, для яких встановлені алгоритми формування на кожному пристрої. Два користувача, які хочуть обмінятися інформацією в різних куточках планети можуть обмінятися номером алгоритму для формування ключа і фразою. В результаті користувачі створять на своїх пристроях однакові ключі і зможуть швидко і просто обмінюватися захищеною інформацією [6, с. 49].

**Список використаних джерел:**

1. Информационная безопасность RUNNet / А.В. Аграновский, А.К. Скуратов // Тр. XI Всеросс. научн.-методич. конф. Телематика 04. – Т. 1. – СПб., 2004. − С. 66-68.

2. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, Р.Е. Серов. – М.: Горячая линия-Телеком, 2002. – 152 с.

3. Дорошенко А.Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах: учебн. пособ. / А.Н. Дорошенко, Л.Л. Ткачев. – М.: МГУПИ, 2006. – 143 с.

5. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: Бак, 2003. – 144 с.

6. Основи інформаційної безпеки / С.В. Кавун, О.А. Смірнов, В.Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.

7. Кузнецов О.О. Захист інформації в інформаційних системах / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.

8. Основи захисту інформації : навч. посібн. / О.А. Смірнов, Л.Г. Віхрова, С.І. Осадчий та ін. – Кіровоград, 2010. – 322 с.

**Ліфашина Д.Є.**
*студент;*
**Прудка Л.М.**
*кандидат психологічних наук, доцент,*
*Одеський державний університет внутрішніх справ*

## ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОФІЛАКТИКИ ПРАВОПОРУШЕНЬ СЕРЕД НЕПОВНОЛІТНІХ

На сучасному етапі розвитку держави серйозну занепокоєність викликають загальнодержавні проблеми сімейного неблагополуччя, криза шкільної та професійної освіти, трудова незайнятість, неорганізованість дозвілля неповнолітніх, наркотизація та ін. В зв'язку з чим, спостерігається динаміка зростання злочинності серед неповнолітніх, яка приймає стійкий рецидивний характер. А таке зростання злочинності лишає суспільство перспектив встановлення соціальної рівноваги і благополуччя.

Сьогодні, перед державою та суспільством, постають питання щодо пошуку шляхів зниження рівня злочинності, в тому числі і серед неповнолітніх. В першу чергу, це можна досягнути, безумовно, ефективно організованою системою заходів профілактичної роботи.

Для цього необхідно вивчити всі існуючі фактори, які обумовлюють правопорушення, і на цій основі побудувати сучасну систему профілактичної діяльності, яка б змогла забезпечити реальне зниження злочинності, в тому числі і серед неповнолітніх.

Курс на профілактику правопорушень – це довготривала орієнтація нашої держави. Найважливішою і кінцевою метою курсу становить викорінення причин і умов, що породжують злочинність серед неповнолітніх. Досягнення поставленої мети забезпечується засобами, які повинні відповідати принципу гуманізму. При цьому слід також наголосити, що профілактична діяльність, і зокрема по відношенню до неповнолітніх, повинна здійснюватись у суворій відповідності з нормами права [1, с. 8].