сім'ї. Первинна профілактика насильства щодо дітей – це сукупність заходів, спрямованих на запобігання розвитку чинників ризику виникнення насильства щодо дітей; формування у суспільстві ненасильницького світогляду, культури толерантності та чуйності (в тому числі гендерної); неприйняття насильницької моделі виховання дітей та насильницьких стосунків між людьми загалом.

Вторинна профілактика насильства щодо дітей це – сукупність заходів, спрямованих на раннє виявлення ситуацій підвищеного ризику виникнення насильства; виявлення, усунення та подолання чинників, які сприяють скоєнню насильства щодо дитини конкретними особами.

Третинна профілактика насильства щодо дітей – сукупність заходів втручання після здійснення насильства, спрямованих на недопущення рецидиву, реабілітацію дитини, яка зазнала насильства та роботу з агресором.

В Україні законодавчо визначено систему установ та організацій, на які покладаються захист дітей від насильства та профілактика цього явища. До цієї системи входять: службу у справах дітей; уповноважені органи Національної поліції (насамперед служба ювенальної превенції); органи та заклади освіти; органи та заклади охорони здоров'я; управління (відділи) у справах сім'ї, молоді та спорту; центри соціальних служб для сім'ї, дітей та молоді; притулки для дітей та центри соціально-психологічної реабілітації дітей; Всеукраїнська дитяча лінія «Телефон Довіри» (0-800-500-21-80) [6, с. 48].

Слід зазначити, що масштаби даного феномену є глобальними, тому від подальшої соціально-психологічної роботи всіх зазначених структур залежить формування соціально-адаптованих людей, здатних створювати повноцінну сім'ю, бути гарними батьками, гідними громадянами своєї держави.

1. Конвенція про права дитини 1989 р. URL:https://zakon.rada.gov.ua/laws/show/995_021
2. Трубавіна І. М. Теоретико-методичні основи соціально-педагогічної роботи з сім'єю: автореф. дис. на здобуття наук. ступеня доктора педагог. наук: спец. 13.00.05 «Соціальна педагогіка». Луганськ, 2009. 46 с.
3. Юрій Вітомський: «Безпека дітей – основа безпеки держави» Урядовий кур'єр. 23 травня 2021.
4. Ткаченко І. М. Теоретико-кримінологічна характеристика факторів, що обумовлюють насильство в сім'ї: Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2013, вип. № 6-1 т. 1. С 80-83.
5. Клочан Ю. В. Соціально-педагогічна профілактика жорсткого ставлення до дітей у сім'ї: Вісник ЛНУ імені Тараса Шевченка, 2014, №5, ч.1. С.84-92.
6. Безпалько О. В. Соціальна робота: Навч. посібник. К., 2004. С.165.

Олександр Шумейко,
старший викладач
кафедри психології та педагогіки
Дніпропетровського державного
університету внутрішніх справ

ПСИХОЛОГО-ОРГАНІЗАЦІЙНА СКЛАДОВА УПРАВЛІННЯ ТА ЗАХИСТУ ІНФОРМАЦІЙНИХ МЕРЕЖ

У сучасному цифровому світі величезне значення приділяється психолого-організаційній складовій захисту інформації в інформаційних системах усіх типів. Інформаційна психологія в результаті вивчення структури інформаційних систем і технологій обробки даних в ній виділяє концепцію інформаційної безпеки, на підставі якої надалі проводяться всі роботи по захисту інформації в інформаційних системах [3]. У концепції знаходять відображення такі основні моменти:

- організація мережі самої організації;
- існуючі загрози безпеці інформації, можливості їх реалізації та завдання шкоди від цієї реалізації;
- організація зберігання інформації в інформаційних системах;
- організація обробки інформації (на яких робочих місцях і за допомогою якого про-

грамного забезпечення);

- регламентація допуску персоналу до тієї чи іншої інформації;
- відповідальність персоналу за дотримання безпеки.

У кінцевому підсумку на основі концепції інформаційної безпеки інформаційних систем створюється схема безпеки, структура якої повинна задовольняти таким умовам:

1. Захист від несанкціонованого проникнення в корпоративну мережу і можливості витоку інформації по каналах зв'язку.
2. Розмежування потоків інформації між сегментами мережі.
3. Захист критичних ресурсів мережі.
4. Захист робочих місць і ресурсів від несанкціонованого доступу.
5. Криптографічний захист інформаційних ресурсів.

З практичного погляду, політику безпеки доцільно розглядати на трьох рівнях деталізації. До верхнього рівня можна віднести рішення, що зачіпають організацію в цілому. Вони носять досить загальний характер і, як правило, виходять від керівництва організації. Приблизний список подібних рішень може включати в себе наступні елементи:

- рішення сформувати або переглянути комплексну програму забезпечення інформаційної безпеки, призначення відповідальних за просування програми;
- формулювання цілей, яких бажає досягти організація в області інформаційної безпеки, визначення загальних напрямків у досягненні цих цілей;
- забезпечення бази для дотримання законів і правил;
- формулювання адміністративних рішень із тих питань реалізації програми безпеки, які повинні розглядатися на рівні організації в цілому.

Політика верхнього рівня мети організації в області інформаційної безпеки формулюється в термінах цілісності, доступності та конфіденційності [3; 4]. Якщо організація відповідає за підтримку критично важливих баз даних, на першому плані може стояти зменшення числа втрат, пошкоджень або спотворень даних. Для організації, що займається продажем комп'ютерної техніки, ймовірно, важлива актуальність інформації про надані послуги і ціни та їх доступність максимальному числу потенційних покупців. Керівництво режимного підприємства в першу чергу піклується про захист від несанкціонованого доступу, тобто про конфіденційність. На верхній рівень виноситься керування захисними ресурсами і координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем, взаємодію з іншими організаціями, що забезпечують або контролюють режим безпеки. Політика верхнього рівня повинна чітко окреслювати сферу свого впливу. Можливо, це будуть всі комп'ютерні системи організації (або навіть більше, якщо політика регламентує деякі аспекти використання співробітниками своїх домашніх комп'ютерів). Можлива, однак, і така ситуація, коли в сферу впливу включаються лише найбільш важливі системи. У політиці повинні бути визначені обов'язки посадових осіб із вироблення програми безпеки та втілення її в життя. У цьому сенсі політика безпеки є основою підзвітності персоналу. Політика верхнього рівня має справу з трьома аспектами законослухняності і виконавської дисципліни. По-перше, організація повинна дотримуватися існуючих законів. По-друге, слід контролювати дії осіб, відповідальних за вироблення програми безпеки. Нарешті, необхідно забезпечити певний ступінь старанності персоналу, а для цього потрібно виробити систему заохочень і покарань. Власне кажучи, на верхній рівень слід виносити мінімум питань. Подібне винесення є доцільним, коли воно обіцяє значну економію коштів або коли інакше вчинити просто неможливо.

Політика безпеки нижнього рівня належить до конкретних інформаційних сервісів. Вона включає в себе два аспекти - цілі та правила їх досягнення, тому її часом важко відокремити від питань реалізації [3]. На відміну від верхнього рівня, зазначена політика повинна бути визначена більш докладно. Є багато речей, специфічних для окремих видів послуг, які не можна єдиним чином регламентувати в рамках всієї організації. У той же час, ці речі настільки важливі для забезпечення режиму безпеки, що пов'язані з ним рішення повинні прийматися на управлінському, а не технічному рівні. Наведемо кілька прикладів питань, на які слід дати відповідь в політиці безпеки нижнього рівня: - хто має право доступу до об'єктів, підтримуваних сервісом? - за яких умов можна читати й модифікувати дані? - як організований віддалений доступ до сервісу? При формулюванні цілей політики нижнього рівня можна виходити з міркувань цілісності, доступності та конфіденційності, але не можна на цьому зупинятися. Її цілі повинні бути більш конкретними. Наприклад, якщо мова йде про систему розрахунку заробітної плати, можна поставити мету, щоб лише співробітникам

відділу кадрів та бухгалтерії дозволялося вводити й модифікувати інформацію. У більш загальному випадку цілі повинні пов'язувати між собою об'єкти сервісу та дії з ними. З цілей виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим докладніші правила, чим більш формально вони викладені, тим простіше підтримати їх виконання програмно-технічними засобами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів, імовірно їх доведеться часто переглядати. Керівництву належить знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а співробітники не виявляться надмірно обтяжені. Зазвичай найбільш формалізуються права доступу до об'єктів, зважаючи на особливу важливість даного питання. Перш ніж будувати якусь систему захисту, визначимо, що й від кого ми хочемо захистити. Не можна захистити все й від усього. Адже не вся інформація для певної установи чи організації є однаково цінною. Для початку потрібно виділити перелік інформації (файлів), які необхідно захистити, і її фізичне розміщення (відразу стане ясно, що захищати краще інформацію, яка зберігається на одному сервері або окремому комп'ютері). Необхідно обміркувати, чим може обернутися простоювання комп'ютерів, втрата електронної пошти за день або втрата важливих даних. Друге, що необхідно розуміти, - від кого ми захищаємо інформацію. Ким є потенційний зловмисник, який тими чи іншими засобами може заволодіти важливою інформацією. Одночасно доцільно оцінити сили зловмисника: які він може мати організаційні або технічні можливості для доступу до інформації (адже зловмисник може бути співробітником організації і діяти зсередини), скільки часу та коштів йому не шкода направити для заволодіння інформацією [3; 4]. Потенційного зловмисника власне може й не бути, а безпеці інформації можуть загрожувати випадкові фактори (технічні вірусні атаки, вихід з ладу комп'ютерів тощо).

Третє, що треба оцінити - це загрози інформації. Розрізняють такі групи загроз:

- несанкціонований доступ до інформації (читання, копіювання або зміна інформації, її підробка, спотворення);
- порушення працездатності комп'ютерів та прикладних програм, що може спричинити зупинку виробничих процесів;
- знищення інформації.

У кожній із цих трьох груп можна виділити десятки конкретних загроз. Варто зазначити, що загрози можуть бути навмисними й випадковими, а випадкові, у свою чергу, обумовлені природними факторами (пожежі, руйнування, стихійні лиха) та людським фактором (помилкові дії персоналу). Випадкові загрози, в яких відсутній лихий задум, зазвичай небезпечні лише можливістю втрати інформації й порушення працездатності системи, від чого досить легко застрахуватися. Навмисні ж загрози більш серйозні з погляду втрат для бізнесу, бо тут доводиться боротися не з нещадно жорстким випадком, а з інтелектуальним противником. З'ясування таких факторів: що, від кого або від чого ми будемо захищати – це вже значний крок на шляху до відповіді на головне питання – як захищати [3]. На цьому шляху психологія є однією із основних наук, яка допоможе дати відповідь на ці та багато інших актуальних питань інформаційної безпеки.

1. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. К.: Видавничо-поліграфічний центр “Київський університет”, 2008. 274 с.

2. Інформаційно-психологічні війни. Проблеми інформаційної незалежності держави. URL: http://vybory.org/articles/485.html

3. Ясенев В.Н., Дорожкин А.В., Сочков А.Л. и др. Информационная безопасность: Учебное пособие. Нижний Новгород. Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. 198 с.

4. Почепцов Г. Информационные войны. Основы военно-коммуникативных исследований. URL: http://www.ligis.ru/librari_2/049/contents.html