© Skyba A., Khorina O. Prediction of social, psychological and situational factors of criminal thoughts and intents activation in information security // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 2, p. 165-173.

ПРОГНОЗУВАННЯ СОЦІАЛЬНО-ПСИХОЛОГІЧНИХ ТА СИТУАЦІЙНИХ ЧИННИКІВ АКТИВАЦІЇ ЗЛОЧИННИХ ДУМОК І НАМІРІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Андрій Скиба[1], Олена Хоріна[2]

[1]Національний технічний університет України «Київський політехнічний інститут», Україна
[2]Інститут соціальної та політичної психології Національної академії педагогічних наук України, Україна

СКИБА Андрій Володимирович

Рік та місце народження: 1990 рік, м. Трускавець, Львівська область, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут», 2007 рік.
Наукові інтереси: інформаційна безпека, інформаційні та фінансові ризики, управління проектами, комплексні системи оцінки ризиків.
E-mail: andrewskyba@ukr.net

ХОРІНА Олена Іванівна

Рік та місце народження: 1968 рік, м. Бровари, Київська область, Україна.
Освіта: Київський національний університет імені Тараса Шевченка, 1993 р.
Посада: молодший науковий співробітник лабораторії моніторингу ІСПП НАПН України, 2005 р.
Наукові інтереси: особистісний розвиток, міжособові стосунки, соціальна ситуація діяльності.
E-mail: olena_khorina@ukr.net

Анотація. *Запропоновано спосіб оцінки інформаційних ризиків та безпеки за допомогою системи прогнозування соціально-психологічних, ситуаційних чинників, які здатні активізувати злочинні наміри. Виявлення типів соціально-психологічної адаптації людини до близького оточення та світу використовується в транзакційному аналізі. Основу системи прогнозування складає опитувальник особистісних адаптацій Вена Джойнса (Joines Personality Adaptation Questionnaire, JPAQ). Він визначає два типи адаптації, зокрема: виживаюча і виконуюча. Виживаюча формується від народження до півтора років, а виконуюча - від півтора років до трьох. Виживаючі адаптації вказують на три несвідомі стратегії пристосування дитини до моделей міжособових стосунків батьків і інших членів родини, відповідно: Творчий мрійник, Чарівний маніпулятор, Блискучий Скептик. Виконуючі адаптації вказують на три несвідомі стратегії, за допомогою яких діти задовольняли очікування оточуючих людей і ігнорували власні бажання. Зокрема: Грайливо-впертий, Відповідальний Трудоголік та Надтореагуючий Ентузіаст. Коли в житті людини "все йде не так" зростає ймовірність застосування ризикових стратегій досягнення бажаного. Неусвідомлені стратегії знаходяться в зоні асоціальних та антисоціальних дій, поза межами правового поля, здорових людських стосунків. Оцінка ймовірності переходу людини в поле досягнення бажаного "будь-якою ціною", відбувається за рахунок визначення провідних особистісних адаптацій. "Перехід" особистості від думок до умовного сценарування злочинного наміру і його реалізації, відбувається в актуальній життєвій/професійній ситуації, яка активізує ризикову мотивацію. Оцінка ймовірного впливу соціально-психологічних та ситуаційних чинників, що не усвідомлюються людиною, здійснюється за допогою блоку ситуаційних запитань. Розширення економіко-вартісної моделі за рахунок системи прогнозування злочинних намірів підвищує оцінку інформаційних ризиків, оптимізує інвестиції в інформаційну безпеку, здійснює аналіз ризиків "переходу" людини від позиції законослухняного громадянина до позиції зловмисника.*

Ключові слова: *інформаційна безпека, оцінка ризиків, економіко-вартісні моделі, особистісні адаптації, соціально-психологічні типи зловмисників, транзактний аналіз, міжособові стосунки, коефіцієнт небезпеки зловмисника.*

Вступ

Управління інформаційною безпекою підприємства передбачає використання актуальної нормативно-правової документації рекомендаційного характеру, що спирається на стандарти ISO 27005 [1] та ISO 31100 [2] і є узагальненням кращих світових практик. Проектування системи захисту/оцінки інформаційної безпеки вимагає уваги до основних діячів, дотичних до управління інформаційними активами. Останні можуть потенційно загрожувати інформаційним активам, бути свідомими/несвідомими провідниками ризиків. Особистість унікальна і неповторна, за сприятливих умов вона створює геніальні рішення для життя й бізнесу, а за несприятливих - робить вчинки, і не може собі пояснити, не розуміє, як була здатна на сумнівний вчинок, під впливом внутрішніх та зовнішніх чинників.

Оцінюючи можливі інформаційні та фінансові ризики в сфері безпеки, варто враховувати особистісні особливості, які пов'язані з цінностями життя й діяльності, оскільки вони регулюють вибір оточення, роботи та стиль вирішення проблемних ситуацій, суттєво впливають на вибір стратегій досягнення бажаного.

В цій статті пропонується розглянути особливості поведінки/міркувань особистості, в залежності від несприятливих умов життя й діяльності. Чинники, які можуть активувати стратегію досягнення бажаного через скоєння злочину в сфері інформаційної безпеки. Прийняття ризикового рішення і його реалізація можуть бути усвідомленим актом або частково усвідомленим, або несвідомим, майже випадковим. Ці нюанси впливають на оцінку ризиків кожного етапу експертизи інформаційної безпеки. Важливо враховувати соціально-психологічні особливості особистості для визначення кількісних показників, що застосовуються в економіко-вартісних моделях [3,4,5] та комплексних системах оцінки інформаційних і фінансових ризиків.

Психологічна наука й практика розглядає особистість як унікальну і цілісну. Навіть, коли людина використовує в житті та/або в професії антисоціальні стратегії досягнення бажаного, психологи розглядають це, як певний дефіцит розвитку, відхилення або особистісний розлад. Виключенням є психічне нездоров'я людини, тобто нездатність усвідомлювати власні мотиви і вчинки, свідомо діяти. Специфіка психологічного та соціально-психологічного підходів полягає в гуманному ставленні до людини. Оцінюються перш за все вчинки, а не особистість. Зокрема, Ерік Берн, засновник методу транзакційного аналізу [6], вважав, що всі люди народжуються "ок", вчинки людей бувають "не ок", а відтак, є можливість за допомогою психологічного консультування або психотерапії допомогти людині відтворити відчуття власної гідності. Саме тому психологи ретельно досліджують обставини, в яких людина зростала і формувалася як особистість, оскільки оточення й традиції виховання мають значний вплив на ціннісні життєві орієнтири, а згодом і на вибір життєвих/ділових стратегій. Якщо в близькому оточенні людини нормою була неповага до себе й інших людей, то повагу до себе така людина ймовірно, здобуватиме за рахунок задоволення потреб інших людей, ігнорування власних. Більшість злочинів люди вчиняють з позиції виправдання очікувань інших людей, або змушення когось догодити їм. Такі люди залишаються поза критичним осмисленням, усвідомленням себе, власних потреб і способів їх прийнятного задоволення в межах суспільного життя. Якщо ж це усвідомлений процес, тоді вартого говорити про антисоціальний розлад особистості.

Для психолога й юриста не екологічно підозрювати людину в скоєнні злочину. Існує презумпція невинності. Якщо є предмет для прогнозу ймовірності скоєння злочину, психологу екологічно оцінювати ризики в сфері інформаціної безпеки, виходячи з розуміння обставин і ситуацій, які можуть активувати не властиву психічно здоровій людині стратегію досягнення бажаного, зокрема через створення задуму, плану та реалізації злочину. Прогнозується ймовірність настання таких ситуацій у внутрішньому й зовнішньому житті/діяльності людини, що спонукають її до зловмисних намірів та дій. Створення інструменту оцінки ризиків і ситуацій професійної взаємодії - важливе завдання для фаховців, в тому числі їхніх дій "на випередження", своєчасне знешкоджування намірів потенційних зловмисників.

Першу спробу розглянути і розрахувати коефіцієнти ризиків в сфері інформаційної безпеки автори відобразили в статті "Розширення економіко-вартісних моделей інформаційних ризиків за рахунок використання соціально-психологічних типів змовмисника" [5]. Типи зловмисників характеризувалися, виходячи з таких критеріїв: 1) мотивація (свідома/несвідома, психологічна/матеріальна); ресурси (власні/запозичені), 3) статус перебування ймовірних злочинців (в організації або за її межами, тощо).

Це дослідження є спробою розробити інструмент прогнозування ситуацій й обставин, які можуть активувати зловмисні стратегії досягнення бажаного працівниками компанії в залежності від їхнього типу адаптацій до життя, близького оточення та різноманітних ситуацій взаємодії з колегами, іншими людьми. Автори статті використали опитувальник особистісних адаптацій Вена Джойнса (Joines Personality Adaptation Questionnaire, JPAQ), транзакційного аналітика [7], який виявляє типи адаптацій. Анкета містить 72 запитання, по 12 на кожну з шести особистісних адаптацій, ключ та керівництво з обробки й інтепретації отриманих даних. Мета використання опитувальника - визначення провідних особистісних

адаптацій для оцінки ймовірності скоєння злочину у сфері інформаційної безпеки, під впливом неусвідомлюваних соціально-психологічних та ситуаційних чинників, які провокують особистість на порушення інформаційної безпеки.

В статті використовуються терміни і визначення, прийняті в методі транзакційного аналізу для пояснення логіки опитувальника. Зокрема: окейність й сценарії життя (Ерік Берн), двері комунікації (Поль Вар), драйвери, міні сценарій, (Тайбі Каллер), особистісні адаптації (Вен Джойнс) [6,7,8,9].

Оскільки психодіагностичні методики не передбачають частину запитань, яка відображає емоційний стан і життєву/виробничу ситуацію респондента на момент опитування, автори створили низку запитань, які відображають актуальну життєву/ділову ситуацію респондента. Додатково можна оцінити обставини життя/роботи респондента, як сприятливі, або несприятливі. За несприятливих обставин життєві й ділові ресурси людини виснажуються швидше, а ризики зростають. Додатковий блок запитань з визначення актуальної життєвої/ділової ситуації респондента надає можливість коригувати коефіцієнти ризиків інформаційної безпеки.

Короткі тези з транзакційного аналізу, методу психотерапії, консультування, який успішно застосовується в сфері освіти й організаційного консультування. Перша теза самого засновника методу Еріка Берна про окейність. Всі люди народжені "ок", а їхні вчинки можуть бути "не ок". З моменту народження людина проходить певний шлях і від багатьох чинників залежить, чи почуває вона себе "ок" незалежно від обставин, чи є володарем ситуаційної окейності. Ерік Берн визначав актуальний стан окейності людей за їхньою життєвою позицією: 1) я-"ок", ти-"ок" - стиль продуктивної співпраці і близьких стосунків; 2) я-"ок", ти-"не ок" - стиль експлуатації ресурсів/інших людей; 3) я-"не ок", ти- "ок" - стиль альтруїзму і жертовності, депресії; 4) я-"не ок", ти-"не ок" - стиль бунтарства та/або соціальної ізоляції. Навіть, якщо людина має життєву позицію "я-ок, ти-ок" і здатна плідно співпрацювати, існує ризик, що вона може опинитися в ситуації, коли інші люди спробують нав'язати їй позицію "ти - ок, якщо відповідаєш нашим вимогам та очікуванням, тож доведи...". Будь-яка стратегія маніпулювання включає компонент нав'язування людині умовної окейності (гідності), і висування вимог, за яких вона має зробити те, що їй не притаманно, не бажано, проти її волі при нав'язаній іллюзії, що це саме і є її бажання, мотивація, тощо. Транзакційні аналітики Поль Вар (Paul Ware) , Тайбі Каллер (Taibi Kahler) та Вен Джойнс (Vann S. Joines) працювали в царині створення понять: "драйвери", "двері комунікації", "міні сценарії", "особистісні адаптації". Зокрема, поняття особистісної адаптації в транзакційному аналізі означає тип створення стосунків з людьми і вирішення проблемних ситуацій життя та діяльності. Типи створення стосунків з людьми бувають активними і пасивними, груповими та/або індивідуальними. Тайбі Каллер розрізняв п'ять видів поведінкових драйверів, як неусвідомлених дій і вчинків, що сформувалися до трьох років. Драйверна поведінка є психологічно обумовленою захисною поведінкою та дістала такі назви: Радуй інших (активно-груповий стиль, аналог істероїдного), Намагайся (пасивно-груповий стиль, аналог пасивно-агресивного), Будь досконалим (активно-індивідуальний стиль, аналог обсесивно-компульсивного) і Будь сильним (пасивно-індивідуальний стиль, аналог шизоїдного), драйвер Поспішай властивий всім. Кожному стилю, який автор назвав драйвером, притаманна певна послідовність комунікативних каналів, таких, як: мислення, емоції та поведінка. Поль Вар вважав, що люди, відповідно до свого стилю мають певну послідовність каналів комунікації, так звані "двері комунікації": 1) відчинені двері, за допомогою яких люди починають комунікацію та взаємодію з іншими, 2) двері-мета, через, які можливий розвиток і продуктивні особистісні зміни, і 3) двері-пастка, через які блокується взаємодія та погіршуються стосунки. Тайбі Каллер показав, що мислення, емоції і поведінка людини з кожного драйверу є неусвідомлюваними і виконують функцію механізму, який допомагає людині реалізовувати несвідомий план життя, що дістав в транзакційному аналізі назву життєвого сценарію. Різновиди драйверної поведінки властиві людям в різних ситуаціях. Наприклад, в родинному житті і в стосунках з друзями переважатиме один стиль, в роботі - інший, а ситуаціях сильного стресу і потрясіння - інші. Вен Джойнс дав розвиток теорії драйверів Тайбі Каллера. По-перше, запропонував використовувати назву "особистісні адаптації" і дав інші визначення, добре зрозумілі людям, впізнавані і здатні сформувати розуміння ресурсів та ризиків кожної адаптації. По-друге, ввів дві адаптації зокрема: антисоціальну - Чаруючий Маніпулятор (поєднання активно-групового стилю та пасивно-індивідуального) та параноїдну - Блискучий Скептик (активно-індивідуальний стиль). В-третє, розробив новий опитувальник, і дав інтерпретації не тільки самим стилям адаптацій, а й їхнім комбінаціям, а їх 37. В-четверте, запропонував використовувати опитувальник, як методичний засіб налагодження комунікацій зі співробітниками в організаціях, роблячи акценти на сильні, ресурсні властивості і зменшуючи ризикові прояви.

Інтерпретація результатів опитування включає коротку характеристику взаємодії співробітника, критерії ризикових ситуацій, на які йде відповідна реакція й прогноз поведінкової стратегії співробітника, якщо йому не вдалося отримати бажаного звичним способом. Власне, зміст ризикової складової кожного стилю адаптації та їхніх комбінацій, взято за основу системи прогнозування ризику ймовірності порушення інформаційної безпеки співробітниками. Разом із блоком запитань, спрямованих на визначення актуальної ситуації життя та діяльності співробітників, як сприятливої або несприятливої, опитувальник особистісних адаптацій Вена Джойнса може використовуватися

разом з іншими відомими методиками, зокрема MMPI аби забезпечити валідність інструментарію.

Отже, опитувальник особистісних адаптацій Вена Джойнса (Joines Personality Adaptation Questionnaire, JPAQ) був вибраний авторами для створення інструменту оцінки ризиків інформаційної безпеки, виходячи з таких аргументів. По-перше, легкий в використанні, по-друге, вказує на тенденції переважання певних стилів адаптації в людини та їхніх комбінацій, втретє, пропонує в якості інтерпретації ресурсні і ризикові особливості особистості, вчетверте, визначає соціально-психологічні й ситуаційні чинники, під впливом яких людина змінює стратегію досягнення бажаного, в-п'яте, визначає вектор цієї стратегії, в-шосте, може бути інтерпретований респонденту з точки зору його особистісного розвитку, продуктивних шляхів, а не з точки зору підозр. Опитувальник може бути використаний департаментом персоналу і службою безпеки для ефективної оцінки ризиків та розробки стратегій інформаційної безпеки.

Раніше розглянута авторами структура економіко-вартісної моделі має розширення за рахунок соціально-психологічних характеристик зловмисника [5]. Також в розширенні моделі запропоновані соціально-психологічні моделі (портрети) зловмисників інформаційної безпеки, які покривають весь спектр можливих сценаріїв розвитку реалізації загроз. Без них оцінка ризиків є неповною, а відтак - неефективною. Виходячи з попередніх досліджень, такі характеристики відсутні в відомих нині моделях.

Визначення соціально-психологічних типів зловмисників на основі особистісних адаптацій Вена Джойнса в сфері інформаційної безпеки

Для оцінки інформаційних ризиків керівник компанії має визначити показники, за якими проводиться оцінка і коло співробітників, які працюють з інформацією. Серед показників виділяють основні чотири: 1) показник стабільності компанії, 2) показник технічної захищеності об'єкта, 3) показник ймовірності реалізації атаки через канал по об'єкту та 4) показник небезпеки зловмисника інформаційної безпеки. Є інші показники, які застосовуються для оцінки інформаційних ризиків, і враховують різні ситуації, сфери діяльності компанії тощо. Найбільш поширеними є вищенаведені чотири показники. Складовою показника небезпеки зловмисника інформаційної безпеки є соціально-психологічні типи зловмисника. Метою статті є обгрунтування значущості розширення показника небезпеки зловмисника для підвищення якості інформаційної безпеки. Завдання статті: обгрунтувати інструмент виявлення соціально-психологічних типів зловмисників і створення прогнозу чинників, які активізують злочинні наміри/дії.

Після визначення показників інформаційної безпеки і окреслення кола осіб, які працюють з інформацією, зі співробітниками працює психолог, співробітник HR-департаменту. Фахівець використовує методичний комплекс опитувальників, додаткову усну бесіду, визначає ймовірність настання ризиків "переходу" працівника з ролі співробітника до ролі зловмисника.

Основу методичного комплексу складає опитувальних особистісних адаптацій Вена Джойнса. Він має опис кожної з 6 особистістних адаптацій та інтерпретацію їхніх комбінацій (37). Кожна з інтерпретацій вказує на декілька параметрів, зокрема: 1) стиль вирішення проблем співробітником, 2) характер створюваних виробничих, міжособових стосунків, 3) ймовірні стратегії реагування людини на стресову ситуацію, 4) тригери/обставини/поведінку інших людей, які можуть активувати ризикову поведінку співробітника.

В результаті виокремлюються чинники, які можуть створювати перехрещення умов активації злочинних думок, намірів і їх реалізації в сфері інформаційної безпеки. Додатково було розроблено коефіцієнти оцінки мотиву помсти з власного імпульсу або зовнішнього, щось на кшталт підказаного мотиву, а також коефіцієнти ймовірності індивідуальної або/чи командної діяльності. Це предметно буде розглянуто в окремій статті.

Стилі адаптації людини формуються в ранньому віці внаслідок певного типу батьківського виховання. Вони формують реакцію малюка на ситуації родинного життя. Якщо сила ситуації перевищує здатність дитини емоційно впоратися з нею і відсутня підтримка батьків й близького оточення, то така ситуація сприймається дитиною, як загроза її життю. Таким чином, формуються певні стилі виживання, які Вен Джойнс назвав адаптаціями виживання. Їх три: Творчий Мрійник (активно-груповий стиль), Блискучий Скептик (активно-індивідуальний) і Чаруючий Маніпулятор (антисоціал, поєднання активно-групового та пасивно-індивідуального стилів). Період їхнього формування: від народження приблизно до півтора року. Адаптації виживання "включаються", коли існує сильна загроза, надмірний стрес, які в сприйнятті малої дитини, а потім, дорослої людини несвідомо переживаються, як загроза життю. Наступні три адаптації формуються в період від півтора до трьох років, як стиль задоволення очікувань батьків й близького оточення. Це такі стилі: Грайливо-Впертий (пасивно-груповий стиль), Відповідальний Трудоголік (активно-індивідуальний) і Надтореагуючий Ентузіаст (активно-груповий стиль).

Розглянемо детально кожну з адаптацій виживання, зокрема: **Творчий Мрійник, Чаруючий Маніпулятор, Блискучий Скептик.**

Творчий Мрійник в сильній стресовій ситуації допомагає людям, забувши про свої потреби, натомість сподівається отримати допомогу, коли все владнається. Очікування його не здійснюються, оскільки домовленості про взаємну допомогу не було. Не отримавши допомоги, Творчий Мрійник фантазує, замінює задоволення потреб іллюзіями. Виснаження його ресурсів

відбувається внаслідок незадоволених власних потреб і використання ресурсів на потреби інших людей. Мотив помсти у Творчого Мрійника може з'явитися в разі жорсткого відхилення його запиту на допомогу. Відчуваючи сильне розчарування, він може несвідомо відгукнутися на пропозицію помсти. Ймовірність помсти з боку Творчого Мрійника низька від 0 до 0,25 за шкалою 0-1, де 0 -неможливо, 1-можливо. Діятиме сам - 0,75 за аналогічною школою, або в складі команди 0,25, за умови мінімальної комунікації. Він здатен зробити "ювелірну" роботу.

Чайручий Маніпулятор – зверне увагу на себе і свої потреби, йому байдуже на потреби інших людей. Якщо він не отримує задоволення власних потреб іншими людьми, то маніпулює, хитрує, залякує, аби змусити їх поступитися. Задовольняє свої потреби будь-якою ціною. Виснаження Чаруючого Маніпулятора відбувається внаслідок незадоволених його потреб шляхом шантажу, тиску тощо. Тоді він створює план помсти і шукає виконавців. Мотивація його - власна, високого рівня від 0,75 до 1, а діятиме командою з аналогічним коефіцієнтом. Наявність високих балів респондента за цим показником має пригорнути пильну увагу департаменту персоналу і служби безпеки. Такі люди несвідомо шукають обмежень, тож варто зрозумілі і тверді обмеження застосувати вчасно. Наприклад, угоду про конфіденційність в роботі з інформаційними ресурсами з детальним описанням наслідків, з вказанням статей карного кодексу і термінів позбавлення волі.

Блискучий Скептик виявляє обережність в стосунках з іншими людьми, аби все правильно зробити й таким чином, уникнути непередбачених обставин. Це його спосіб контролювати ризики. Якщо запропонована стратегія не приймається, Блискучий Скептик стає підозрілим, критичним, наполягає на своєму. Йому варто доручати роботу з виявлення недоліків, підготовки кращих варіантів вирішення проблем. Мотивація помсти можлива (0,5-1), власна, психологічна за змістом. Діятимуть самі і з командою, в залежності від обставин. Вміють добре організувати справу і блискуче довести її до завершення. Самі по собі Блискучі Скептики безпечні, варто приділити увагу комбінаціям адаптацій разом з Чаруючим Маніпулятором, Відповідальним Трудоголіком та Надтореагуючим Ентузіастом.

Комбінації виживаючих адаптацій: Творчий Мрійник і Чаруючий Маніпулятор. Людина з двома означеними адаптаціями схильна до хитрування в стосунках з людьми. Назовні погодиться з бажаннями іншої людини, але потім, таємно, зробить своє, ігноруючи інтереси інших людей. Стратегія – погоджуючись, приспати пильність і реалізувати свій задум будь-якою ціною. «Переможців не судять» - ось їх гасло. Мотивація помсти ймовірна, власна. Можуть діяти самі, з командою, за обставинами. Поєднання двох адаптацій виживання: Творчий Мрійник і Блискучий Скептик легко визначити за стратегією підтримки інших в обмін на підтримку їхнього рішення. В зворотному випадку, буде лють і настирливі спроби змусити інших робити те, що він вважає правильним. Вирогідність помсти висока, власна мотивація, діятимуть командою.

Людина з двома адаптаціями Чаруючий Маніпулятор і Блискучий Скептик, схильна виявляти нарцисичні риси (низьку самооцінку на фоні нереалістичних амбіцій). Спочатку вона намагається виглядати блискучою і кращою порівняно з іншими. Якщо її переваги не визнані, вона відчуває себе вразливою і роздратованою на інших або впадає у лють. Ймовірність мотиву помсти висока, власна, діятиме здебільшого командою, яку легко збере з кращих професіоналів.

Розглянемо детально кожну з виконуючих адаптацій, зокрема: **Грайливо-впертий, Відповідальний Трудоголік, Надтореагуючий Ентузіаст.**

Людина з адаптацією **Грайливо-Впертого** буде наполегливою та непохитною у своїх спробах отримати бажане. Вона намагається щось робити, а не діяти результативно. Зазвичай вона ниє, скаржиться, поводиться безпорадно або канючить, поки інша людина не поступиться. Якщо її спосіб отримати бажане, не допомагає, вона впираються і саботує співпрацю, ігнорує бажання інших людей. Вони гарно виступають в ролі лідерів опозицій, коаліцій. Ймовірність мотиву помсти надто висока, мотив власний, легко зберуть команду невдоволених і того, хто її успішно очолить, самі будуть надихати і привласнювати лаври.

Людина з адаптацією **Відповідального Трудоголіка** орієнтована на досягнення, сподівається, отримати гідне і поважне ставлення бездоганною роботою. Прагне бути надто відповідальною стосовно інших. Якщо стратегія досягнень не допомагає відчути себе коханою і значущою у відносинах, вона думає: «Може, якщо я зроблю щось ще, тоді мене гідно оцінять». Згодом весь її час зайнятий роботою. Її намагання бути досконалою вміло експлуатується Чаруючими Маніпуляторами. Відсторонюються, коли багато вкладають сил, а їх знецінюють і критикують. Ймовірність мотиву помсти низька, мотивація - власна і зовнішня, якщо діятимуть, то здебільшого самі. В критичній ситуацій можуть несвідомо відгукнутися на підказаний мотив помсти.

Людина з адаптацією **Надтореагуючий Ентузіаст** спочатку демонструватиме емоційну чуйність до інших, маючи надію зробити їх щасливими натомість отримати багато уваги до себе. Коли така стратегія не допомагає відчути себе значущою, вона перебільшуватиме свої почуття в негативному ключі, змушуватиме інших звернути увагу. Схильна до завдання болісної помсти, мотивація психологічна. Легко організує людей навколо себе, особливо задля помсти. Діятиме командою, але в разі перехоплення влади кимсь, може кинути справу на півдорозі.

Якщо людині одночасно властива адаптація **Грайливо-Впертого і Відповідального Трудоголіка**, вона схильна до коливань між продуктивною роботою і боротьбою. Замість

обрання легких способів виконання завдань, вона занурюється в деталі і ускладнює все або залучається до непотрібної боротьби за владу. Мотивація помсти висока, власна і зовнішня, діятиме коливаючись, то сама, то з командою.

Якщо людині притаманні адаптації **Грайливо-Впертого і Надтореагуючого Ентузіаста**, вона має багато позивної енергії, але легко піде на конфлікт, після критики втягнеться в боротьбу за владу. Від веселощів і задоволення в спілкуванні з іншими людина переходить до сварок і агресії. Ймовірність мотиву помсти надто висока, власна і зовнішня, діятимуть командою.

Якщо людні одночасно притаманні адаптації **Відповідального Трудоголіка і Надто реагуючого Ентузіаста**, вона прагне радувати інших, все робити добре у стосунках. Якщо вона відчуває себе не визнаною і знеціненою, буде сумлінно працюватиме і відчуватиме емоційно пригніченою в стосунках. Вирогідність мотивації помсти середня, власна, діятиме, і з командою, і сама за обставинами.

Розглядати різні комбінації виживаючих та виконавчих адаптацій в межах цієї статті неможливо, їх - 37. Варто користуватися керівництвом до опитувальника [7]. Акцентуємо, що люди з індивідуальним стилем адаптацій (Творчий Мрійник, Блискучий Скептик, Відповідальний Трудоголік) будуть здебільшого діяти самі, а з груповим - (Чаруючий Маніпулятор, Надто реагуючий Ентузіаст, Грайливо-Впертий) діятимуть в групі. Якщо комбінація адаптацій така, що поєднує індивідульні та групові профілі адаптацій, то можна говорити, що стилі діяльності чергуватимуться залежно від ситуації.

Співставимо особистісні адаптації з типами зловмисників інформаційної безпеки, відповідно до їхніх соціально-психологічних характеристик [5]. В нижченаведеній таблиці запропоновано бачення, до якого типу зловмисника може бути спрямована особистіна адаптація або їхні комбінації.

Блок запитань, спрямований на визначення актуальної ситуації життя та діяльності респондента на момент опитування важливий з декількох підстав. Обмеження багатьох тестів й опитувальників полягає в тому, що вони не фіксують ситуаційних чинників, що справляють вплив на людину в процесі опитування. В залежності від багатьох факторів людина може по-різному відповідати на запитання опитувальника.

Таблиця 1

Співвіднесення особистісних адаптацій до соцально-психологічних типів зловмисника

Особистісні адаптації	**Соціально-психологічні типи зловмисників**
Творчий Мрійник	Аутсайдери: Аутсайдер-найманий професіонал, Інсайдер/аутсайдер–шкідник, Інсайдер/аутсайдер–«свояк», Інсайдер/аутсайдер–ненавмисний; Інса́йдер–незадоволений шкідник, Інса́йдер – випадковець, Інса́йдер–ненавмисний

Закінчення таблиці 1

Чаруючий Маніпулятор	Аутсайдери: Аутсайдер-найманий професіонал, Аутсайдер–самозайнятий професіонал, Аутсайдер–менеджер власного угрупування, Аутсайдер–менеджер організованого угрупування; Інсайдери-аутсайдери: Інсайдер/аутсайдер – шкідник, Інсайдер/аутсайдер–«свояк», Інсайдери: Інсайдер–зловмисник
Блискучий Скептик	Аутсайдер-найманий професіонал, Аутсайдер–самозайнятий професіонал, Аутсайдер–менеджер власного угрупування, Аутсайдер–менеджер організованого угрупування; Інсайдери-аутсайдери: Інсайдер/аутсайдер–шкідник, Інсайдер/аутсайдер–«свояк»; Інсайдери: Інса́йдер–незадоволений шкідник
Грайливо-впертий	Аутсайдери: Аутсайдер-найманий професіонал,Інсайдери-аутсайдери: Інсайдер/аутсайдер – шкідник, Інсайдер/аутсайдер– «свояк»; Інса́йдер – ненавмисний
Відповідальний Трудоголік	Аутсайдери: Аутсайдер-найманий професіонал; Інсайдери-аутсайдери: Інсайдер/аутсайдер–шкідник, Інсайдер/аутсайдер–«свояк»; Інсайдери: Інса́йдер–незадоволений шкідник, Інса́йдер – випадковець,
Надтореагуючий Ентузіаст	Аутсайдери:Аутсайдер– менеджер власного угрупування, Аутсайдер–менеджер організованого угрупування; Інсайдери-аутсайдери: Інсайдер/аутсайдер–шкідник, Інсайдер/аутсайдер–«свояк», Інсайдер/аутсайдер–ненавмисний;Інсайдери: Інса́йдер–незадоволений шкідник, Інса́йдер – випадковець

Тому було вирішено описати актуальну ситуацію життя/діяльності, через низку запитань. Тоді коректно говорити, що за такої ситуації людина саме таким чином відповідає. Якщо ситуація зміниться, то і результати тесту можуть змінитися. Мета цього блоку запитань - визначити коригуючий коефіцієнт, який дозволяє оцінити ризик інформаційної безпеки, як вищий або нижчий щодо конкретного співробітника. Відповіді на запитання блоку оцінюються за шкалою від 0 до 1, де 0-не існує ризику, 1-ризик можливий.

Завдяки опитувальнику особистісних адаптацій Вена Джойнса, блока уточнюючих запитань, усної бесіди з психологом, спеціалісти служби безпеки визначають потенційний соціально-психологічний тип зловмисника інформаційної безпеки і оцінюють ризики активізації злочинного наміру/дії. За комплексної оцінки стану захищеності компанії це дає змогу попереднього виявлення небезпечного або можливо небезпечного співробітника компанії або справжнього/ "прогнозованого" зовнішнього/ внутрішнього зловмисника, можливі стратегії активації і розвитку злочинних намірів співробітника.

Для компанії це має позитивний вплив, оскільки дозволяє коригувати систему в середині компанії та досягати кращих результатів управління. Ефективним є розгляд стратегій, необхідних менеджерам, управляючим інформаційними активами компанії. Для економіко-вартісних моделей та комплексної оцінки інформаційної безпеки, запропонований підхід дає можливість отримати не тільки соціально-психологічні типи зловмисника, але і кількісні оцінки співробітників компанії, що критично необхідні для повної оцінки інфоризиків у компаніях.

Таблиця 2

Інструкція до блоку ситуаційних запитань

“Шановний, Колего! Пропонуємо Вам низку запитань стосовно актуальних подій Вашого життя й роботи. Будь-ласка, обведіть колом варіант відповіді або поставте знак “пташки” поряд з відповідним номером. Обирайте варіант, комфортний для Вас”;		
№	Запитання	Варіанти відповіді
1	Маєте неоднозначну ситуацію в житті/на роботі, яка довгий час не вирішується і викликає напруження ?	1) так (0,5); 2) ні (0); 3) ситуативно - так, а взагалі - ні (0,25); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
2	Маєте стабільне джерело доходів?	1) так (0); 2) ні (0,5); 3) ситуативно - так, а взагалі - ні (0,25); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
3	Маєте близького родича та/або дитину, що довго хворіє?	1) так (0,5); 2) ні (0); 3) ситуативно - так, а взагалі - здоровий (а) (0,25); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
4	Ви забезпечені власним житлом?	1) так (0); 2) ні (0,5); 3) ситуативно - так, а взагалі - ні (0,25); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
5	Вистачає Вам особисто грошей на всі потреби?	1) так (0); 2) ні (0,5); 3) ситуативно - так, а взагалі - ні (0,25); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
6	Вистачає грошей Вашій родині?	1) так (0); 2) ні (0,5); 3) ситуативно - так, а взагалі - ні (0,25); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
7	Маєте кредит в банківській або інший фінансовій установі?	1) так (0,25); 2) ні (0); 3) ситуативно - так, а взагалі - ні (0,15); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
8	Приймаєте на момент відповіді на ці запитання лікарські препарати?	1) так (0,25); 2) ні (0); 3) ситуативно - так, а взагалі - ні (0,15); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
9	Маєте мрію, яку складно реалізувати на сучасному етапі життя ?	1) так (0,25); 2) ні (0); 3) ситуативно - так, а взагалі - ні (0,15); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);
10	Можете собі дозволити відпочивати, коли захочете?	1) так (0); 2) ні (0,5); 3) ситуативно - так, а взагалі - ні (0,25); 4) ваша відповідь _____(0,15 балів, в разі зрозумілої змістовної відповіді);

Закінчення таблиці 2

Визначення кількісних оцінок соціально-психологічних типів зловмисників на основі особистісних адаптацій Вена Джойнса в сфері інформаційної безпеки

Для визначення кількісних оцінок кожного соціально-психологічного типу зловмисника в сфері інформаційної безпеки потрібно зрозуміти, що оцінка проводиться в колективах для виявлення ресурсних/ризикових стратегій поведінки співробітників, потенційних/актуальних зловмисників. Колектив формується з особистостей, тому перш за все особистість, яка приймає учать у визначенні загального стану захищеності компанії, розглядається як потенційно ймовірний зловмисник компанії, який на момент проведення оцінки володіє певними соціально-психологічними характеристиками та знаходиться в певній актуальній життєвій ситуації. За допомогою теста Вена Джойнса визначається адаптація особистості, що відображає її соціально-психологічні характеристики, сформовані в ранні періоди життя. За допомогою блоку додаткових запитань визначається актуальна життєва ситуація особистості на момент проведення оцінки. Визначення актуальної ситуації дає можливість прогнозувати підсилюючий або зменшуючий вплив на ймовірність виникнення злочинного наміру співробітника. Опитувальник Вена Джойнса дає картину комбінацій особистісних адаптацій співробітника і інтерпретацію, яка міститься в керівництві до методики. Пройшовши тест Вена Джойнса отримуємо кількісні оцінки за шістьма адаптаціями, згідно керівництва проводимо відокремлення домінуючих адаптацій, визначаємо комбінації адаптацій та проводимо аналіз результатів, тобто за допомогою керівництва інтерпретуємо кількісні показники по кожній з адаптацій, після чого проводимо аналіз зони ресурсів та ризиків. Провівши інтерпритацію та аналіз, для кожної адаптації або комбінації адаптацій отримуємо кількісну оцінку, яка описана в другому розділі цієї статті. Виходячи з кількісних показників зловмисника отримуємо верхню та нижню межу оцінки соціально-психологічного типу особистості за адаптаціями Вена Джойса [0,1]. Де 0 - ймовірність протиправних дій наближається до нуля, 1 - ймовірність активізації злочинних намірів максимально висока. Також як, зазначалося в другому розділі, враховуються ймовірний стиль діяльності зловмисника: 1) діятиме самостійно; 2) діятиме в команді. Будь-який працівник компанії,

має ймовірність активізації зловмисних намірів більшу від 0, оскільки несвідомо може зробити помилку. Блок запитань, спрямованих на визначення актуальної життєвої ситуації особистості, складає 10 запитань. Кожному з них присвоєна кількісна оцінка, яка відображена біля варіантів відповіді. Запитання за значущістю актуальної життєвої ситуації проранжовані, їм додатково присвоєна вага. Так, запитанням 1-3 відповідає вага k_1=0,85, запитанням 4-7 відповідає вага k_2=0,65, та питанням 8-10 відповідає вага k_3=0,4, шкала вимірювання для ваг запитань [0,1]. Відповівши на всі запитання, результат опитування про актуальну ситуацію обчислюється за наступною формулою:

$$AS = 1 - \sum_{k=1,\, m=1}^{n} (1 - Q_k \cdot k_m), \qquad (1)$$

де Q - кількісна оцінка запитання виходячи з відповіді опитувальника про актуальну ситуацію, k - показник важливості, що відповідає конкретному запитанню, Q_k*k_m – результуюча оцінка по кожному з запитань.

В результаті опитування для кожної особистості формується набір з двох кількісних параметрів - кількісний параметрів VD, "адаптація за Веном Джойнсом" та кількісний параметр AS, "актуальна ситуація" на сьогоднішній день. Для отримання комплексного кількісного значення проведемо адитивну звертку двох параметрів:

$$W = p_1 VD + p_2 AS, \qquad (2)$$

де p_1 та p_2 – пріорітети оцінок, в базовому варіанті розгалянуто p_1=0,65 та p_2=0,35, але в залежності від компанії і колективу p_1 і p_2 можуть змінюватися, так як актуальна ситуація може більше впливати на розвиток стратегії співробітників ніж особливості самої особистості в деяких компаніях.

Результатом проведення адитивної звертки результатів соціально-психологічного тестування є кількісна оцінка соціально-психологічних особливостей кожного співробітника компанії, яка також називається коефіцентом небезпеки зловмисника виходячи з його соціально-психологічних особливостей. Вона може використовуватися для ефективного управління людськими ресурсами, покращення комунікації в компанії, підвищення продуктивності праці, і для кількісної оцінки ризиків активізації злочинних намірів співробітників в сфері інформаційної безпеки. За допомогою цієї кількісної оцінки можна оптимізувати бюджет на особистісний/професійний розвиток співробітників, покращення їх *кpi*-показників, створення кадрового резерву тощо. Це водночас знизить ризики активізації злочинних намірів, а відтак, слугуватиме ефективною профілактикою інформаційної безпеки підприємства. Підприємство, яке створює оптимальні умови для продуктивної праці співробітників, інвестує в розвиток людських ресурсів і сучасних технологій, меншою мірою витрачає бюджет на контроль, хоча і він важливий.

Висновок

Система прогнозування інформаційних ризиків, в основі якої є оцінка соціально-психологічних особливостей особистості дає можливість в різні моменти часу виявляти ймовірність активації злочинних намірів/дій співробітників компанії. А також стратегії крадіжки інформації, зокрема: індивідуально або командою, прогнозувати можливі ролі кожного учасника процесу. З іншого боку система дає можливість побудови стратегій особистісного й професійного розвитку співробітників за умови їхньої зацікавленості.

Опитувальник особистісних адаптацій Вена Джойнса допомогає визначити шість особистісних адаптацій людини до оточуючих людей і світу, а також: 1) стиль вирішення проблем співробітником, 2) характер створюваних виробничих, міжособових стосунків, 3)ймовірні стратегії реагування людини на стресову ситуацію, 4) тригери/обставини/ поведінку інших людей, які можуть активувати ризикову поведінку співробітника. Виходячи з цього, можемо прогнозувати два параметри: ймовірність мотивації помсти і стиль реалізації злочинного наміру індивідуальний та/або груповий. Для кожної адаптації та багатьох варіантів комбінацій розроблено бальні оцінки за шкалою від 0 до 1. Таким чином створено інструмент оцінки ризиків.

Створено блок ситуаційних запитань з варіантами відповіді за шкалою від 0 до 1. Запитання характеризують ситуацію життя/роботи респондента, яка може підвищувати аби знижувати ризики втрати інфомації. Кожне запитання має власну вагу і разом із бальними оцінками відповідей створюють коригуючий коефіцієнт.

Запропонований підхід дає можливість визначати, аналізувати та прогнозувати зміни в соціально-психологічних особливостей людини, відповідно до актуальної ситуації. Всі зміни запропоновано представляти в кількісній оцінці, яка дозволяє використовувати дані в різних комплексних системах інформаційної безпеки. Показує динаміку соціально-психологінчих особливостей співробітників, що впливає на якість інформаційної безпеки підприємства, і підприємтсво в цілому.

Вагома перевага представленого підходу стосовно аналізу співробітників компанії, є інтеграція такого процесу для відділу кадрів з ефективним методом підбору персоналу, визначення мотивації кожного співробітника і його стратегій в компанії.

Подальші наукові розвідки в сфері інформаційної безпеки заплановані в напрямі інтеграції оцінки соціально-психологічних особиливостей особистості в комплексну модель оцінки інформаційних та фінансових ризиків в області інформаційної безпеки [3,4,5].

Література

[1] ISO/IEC 27005 — Information security risk management.

[2] BS 31100:2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000.

[3] Архипов О.Є., Скиба А.В. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації (стаття) // Захист інформації. – 2012. – Том15, №4. – С.366 – 375.

[4] Arkhypov O., Skyba A. (2014), «Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models». The Advanced Science Journal, Vol. 12, pp. 75-82.

[5] Архипов О.Є., Скиба А.В., Хоріна О.І. Розширення економіко-вартісних моделей інформаційних ризиків за рахунок використання соціально-психологічних типів зловмисника. // Захист інформації 17 (1). – 2015. – С. 60-72.

[6] Берн Е. Трансактный анализ. – М.: Академический проспект; Трикста, 2004. – 192 с. – С. 88.

[7] Joines Personality Adaptation Questionnaire, JPAQ. – http://seinstitute.com/jpaq

[8] Paul Ware «Doors to Therapy». Transactional Analysis Journal, 1983, №1, p.11-19.

[9] Taibi Kahler «The Process Therapy Model - The Six Personality Types With Adaptations» - http://www.kahlercommunications.com.

УДК 004.056 (045)

Скиба А.В., Хорина Е.И. Прогнозирование социально-психологических и ситуационных факторов активации преступных мыслей и намерений в сфере информационной безопасности

Аннотация. *Предложен способ оценки информационных рисков и безопасности с помощью системы прогнозирования социально-психологических, ситуационных факторов, которые способны активизировать преступные намерения. Выявление типов социально-психологической адаптации человека к близкому окружению и мира используется в транзакционном анализе. Основу системы прогнозирования составляют опросник личностных адаптаций Вена Джойнс (Joines Personality Adaptation Questionnaire, JPAQ). Он определяет два типа адаптации, в частности: выживая и исполняющая. Выживая формируется от рождения до полутора лет, а исполняющая - от полутора лет до трех. Выживая адаптации указывают на три бессознательные стратегии приспособления ребенка к моделям межличностных отношений родителей и других членов семьи, в соответствии Творческий мечтатель, Волшебный манипулятор, Блестящий Скептик. Исполняющие адаптации указывают на три бессознательные стратегии, с помощью которых дети удовлетворяли ожидания окружающих людей и игнорировали собственные желания. В частности: Игриво-Упрямый, Ответственный Трудоголик и Слишком Реагирующий Энтузиаст. Когда в жизни человека «все идет не так» возрастает вероятность применения рисковых стратегий достижения желаемого. Неосознанные стратегии находятся в зоне асоциальных и антисоциальных действий, вне правового поля, здоровых человеческих отношений. Оценка вероятности перехода человека в поле достижения желаемого «любой ценой», происходит за счет определения ведущих личностных адаптаций. «Переход» личности от мыслей к условным сценариям преступного умысла и его реализации, происходит в актуальной жизненной/профессиональной ситуации, которая активизирует рисковую мотивацию. Оценка вероятного влияния социально-психологических и ситуационных факторов, не осознаются человеком, осуществляется с помощью блока ситуационных вопросов. Расширение экономико-стоимостной модели за счет системы прогнозирования преступных намерений повышает оценку информационных рисков, оптимизирует инвестиции в информационную безопасность, осуществляет анализ рисков «перехода» человека от позиции законопослушного гражданина позиции злоумышленника.*

Ключевые слова: *информационная безопасность, оценка рисков, экономико-стоимостные модели, личностные адаптации, социально-психологические типы злоумышленников, транзактный анализ, межличностные отношения, коэффициент опасности злоумышленника.*

Skyba A., Khorina O. Prediction of social, psychological and situational factors of criminal thoughts and intents activation in information security

Abstract. *In this paper proposed a method of evaluetion of information risk and a system of forecasting of social-psychological, situational factors, which are able to activate malicious intent. For identifing of the types of social and psychological adaptation of close environment and the world, authors propose to use transactional analysis. The basis of the forecasting system is a questionnaire of personal adaptations proposed by V. Joines (Joines Personality Adaptation Questionnaire, JPAQ). When in a person's life, «everything goes wrong» it increases the probability of using risk strategies to achieve the desired. Unconscious strategy are in the zone of asocial and antisocial actions outside the legal framework, healthy human relationships. Estimation of transition is in the field of achieving the desired «at any cost» is due to the definition of leading personal adaptations. «Transition» identity of views to the contingent scenarios of criminal intent and its implementation occur in actual life/professional situation that activates risk motivation. Assessment of the likely impact of socio-psychological and situational factors that are not understood by person, carried out by additional unit situational questions. The extension of economic cost models by the forecasting system of criminal intentions improves assessment of information risks, optimizes investments in information security, risk analyzes «transition» of rights of law-abiding citizen position to the position of the attacker.*

Key words: *information security, risk assessment, economic and cost models, personal adaptation, social and psychological types of attackers, transactional analysis, interpersonal relations, a danger or risk of attacker.*

Отримано *19 травня 2015 року*, затверджено редколегією *3 червня 2015 року*