Інформаційна безпека

УДК 343.98

Щербина Діана Стефанівна
Державний науково-дослідний інститут спеціального зв'язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Щербина Диана Стефановна
Государственный научно-исследовательский институт специальной связи и защиты информации Государственной службы специальной связи и защиты информации Украины
Shcherbina Diana
State Research Institute of Special Communications and Information Protection State Service for Special Communications and Information Protection of Ukraine

Лабутін Максим Олегович
Державний науково-дослідний інститут спеціального зв'язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Лабутин Максим Олегович
Государственный научно-исследовательский институт специальной связи и защиты информации Государственной службы специальной связи и защиты информации Украины
Labutin Maksym
State Research Institute of Special Communications and Information Protection State Service for Special Communications and Information Protection of Ukraine

Коваленко Андрій Сергійович
Державний центр кіберзахисту та протидії кіберзагрозам
Державної служби спеціального зв'язку та захисту інформації України
Коваленко Андрей Сергеевич
Государственный центр киберзащиты и противодействия киберугрозами
Государственной службы специальной связи и
защиты информации Украины
Kovalenko Andrii
State Center for Cyber Defense and Counteraction to Cyber Threats of the State
Service for Special Communications and Information Protection of Ukraine

ЯК ВПЛИВАЄ ЛЮДСЬКИЙ ФАКТОР, ПРИ ПРОЕКТУВАННІ КСЗІ, НА ЯКІСТЬ СИСТЕМИ

Анотація. *Розглянуто вплив людського фактору на проектування, побудову та функціонування комплексної системи захисту інформації, а також на інформаційні системи загалом. Беручи до уваги актуальність даної проблеми, ми спробували розрахувати та оцінити втому людини не звертаючись до методів статистичного дослідження.*

Ключові слова: *інформаційна безпека, кібербезпека, автоматизована система, комплексна система захисту інформації, захист інформації, людський фактор, аналіз загроз, ризики, оцінка втоми, проектування системи захисту, комп'ютерні технології, інформаційна система, побудова інформаційної системи.*

Аннотация. *Рассмотрено влияние человеческого фактора на проектирование, построение и функционирования комплексной системы защиты информации, а также на информационные системы в целом. Принимая во внимание актуальность данной проблемы, мы попытались*

рассчитать и оценить усталость человека не обращаясь к методам статистического исследования.

Ключевые слова: *информационная безопасность, кибербезопасность, автоматизированная система, комплексная система защиты информации, защита информации, человеческий фактор, анализ угроз, риски, оценка усталости, проектирование системы защиты, компьютерные технологии, информационная система, построение информационной системы.*

Summary. *The influence of the human factor on the design, construction of the functioning of an integrated information security system, as well as on information systems in general, is considered. Taking into account the relevance of this problem, we tried to calculate and estimate the person's fatigue without resorting to statistical research methods.*

Key words: *information security, cyber security, automated system, complex information security system, information protection, human factor, threat analysis, risks, fatigue estimation, security system design, computer technologies, information system, information system construction.*

Вступ

Актуальність роботи. Ключовим моментом захисту інформації є її поділ на категорії. Залежно від ступеня цінності інформації вибираються і різні процедури її захисту. На сьогоднішній день фахівцями в галузі комп'ютерних технологій розроблено безліч правил і алгоритмів захисту інформації, в тому числі в мережах передачі даних. Таке різноманіття варіантів побудови інформаційних систем породжує необхідність створення різних систем захисту, що враховують індивідуальні особливості кожної з них, в тому числі людський фактор. У той же час, значний обсяг наявних публікацій навряд чи може сформувати чітке уявлення про те, як же підійти

до створення комплексної системи захисту інформації (КСЗІ) для конкретної інформаційної системи, з урахуванням властивих їй особливостей, особливостей кожного працівника, умов функціонування та умов праці. Захист інформації має забезпечуватися комплексом взаємопов'язаних заходів: правових, організаційних, оперативних, технічних, програмних, криптографічних, психологічних та інших. Ступінь впливу заходів тієї або іншої групи на різні загрози інформації не є однаковим. Він залежить від характеру загрози, характеристик середовища, в якому ця загроза може здійснюватися, особистості та мотивів порушника, ділових і моральних якостей співробітників, що беруть участь в обслуговуванні комп'ютерної системи. Через це неабияку цікавість має людський фактор при проектуванні КСЗІ, взаємного впливу інтересів власника інформації, загроз інформації та заходів протидії цим загрозам. Тому людські та організаційна чинники взаємного впливу зазначених вище факторів є досить важливою у теоретичному і в практичному плані – як спосіб оптимізації структури КСЗІ та більш ефективного розподілу коштів, що витрачаються на проведення заходів щодо захисту інформації. Необхідно відповісти на питання, що захищати, від кого і як, скільки потрібно витратити коштів і часу та яка ефективність витрачених ресурсів? Труднощі об'єктивного підтвердження ефективності КСЗІ полягають у недосконалості існуючої в нашій державі нормативної бази. Фахівці відзначають, що людський фактор, за останній рік, суттєво не понизився і тому існує, як один із джерел інцидентів у інформаційній безпеці. Хоч людина і має величезну роль у захисті інформації, але також це слабка ланка в безпеці інформації та кібербезпеці.

Мета даної статті - аналіз людського фактору в області інформаційної безпеки, а саме при побудові комплексної системи захисту інформації (КСЗІ).

1. Комплексна система захисту інформації

Комплексна система захисту інформації (КСЗІ) — взаємопов'язана сукупність організаційних, інженерних та технічних заходів, засобів і методів захисту інформації для забезпечення безпеки інформації.

Критерії інформаційної безпеки: цілісність, конфіденційнітсь, доступність.

Організаційний захист інформації — комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ.

Криптографічний захист інформації — вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключів) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства, попередження несанкціонованої модифікації, попередження несанкціонованого її розголошення.

Інженерний захист інформації — попередження руйнування носія інформації внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

Для забезпечення ТЗІ створюється комплекс технічного захисту інформації, який є складовою КСЗІ.

Під НСД розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Несанкціонований доступ може здійснюватись як з використанням штатних засобів, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

2. Людський фактор, як невід'ємна складова

Людські та організаційні чинники можуть бути пов'язані з інформаційною безпекою.

Фактори, що впливають на безпеку комп'ютера діляться на дві категорії, а саме людський фактор і організаційний фактор. Людські чинники є важливими, тому їх розділяють на групи[2]:

- фактори, які відносяться до управління, а саме робоче навантаження і неякісна робота персоналу;
- фактори, пов'язані з кінцевим користувачем.

Далі ми зосередимося на чотирьох людських факторах, які мають серйозні наслідки впливу на поведінку користувачів.

1. Низька мотивація

Керівництво повинно визначати, що мотивує їх персонал.

2. Недолік обізнаності

Недолік обізнаності пов'язаний з відсутністю загальних знань про об'єкт, де працює співробітник. Вони не можуть захистити себе від крадіжки особистих даних, а також як контролювати доступ інших користувачів до їх комп'ютера.

3. Переконання

Прикладами ризикованого переконання є наступні: вважається, що установка антивірусного програмного забезпечення вирішує проблеми щодо захисту інформації.

4. Безграмотне користування технологіями

Навіть найкраща технологія не може досягти успіху у вирішенні проблем інформаційної безпеки без безперервного людського співробітництва та ефективного використання цієї технології. Ризики в області комп'ютерної безпеки можна класифікувати декількома способами: перевищення привілеїв, помилки та упущення, відмова в обслуговуванні,

соціальна інженерія, несанкціонований доступ, розкрадання особистих даних, фішинг, шкідливі програми і несанкціоновані копії.

3. Основні поняття та визначення

Будь яка велика інформаційна система не може повністю працювати автоматично. Завжди будуть операції для яких процес автоматизації є досить дорогим для організації. Тому, чим більше таких операцій, особливо в основному технологічному ланцюзі роботи КСЗІ, тим більше вона буде залежати від індивідуальних властивостей людини. Виокремимо ряд типових характеристик людини, яка взаємодіє з КСЗІ та від яких залежить її здатність приймати рішення в штатних та аварійних ситуаціях при проектуванні та експлуатації КСЗІ: здатність до адаптації, здатність до втоми, здатність до відпочинку, можливість здійснення помилки, здатність приймати рішення, здатність до запам'ятовування інформації, здатність переносити інформаційне перевантаження, здатність до навчання[1].

Розглянемо кількісну оцінку впливу людського фактору на таку важливу властивість, як доступність (коефіцієнт готовності) КСЗІ.

Коефіцієнт готовності $К_г$ – ймовірність того, що система виявиться в працездатному стані в будь-який момент часу. Дана комплексна характеристика безвідмовності та ремонтопридатності системи, яка характеризується показниками ремонтопридатності: $Т_в$ – середній час наробітку до відмови; $Т_{відн}$ – середній час відновлення після відмови.

Коефіцієнт готовності визначається як:

$$К_г = \frac{Т_в}{Т_в + Т_{відн}}$$

Доступність (D), зазвичай, на відмінно від коефіцієнта готовності виражається у відсотках або $D = К_г * 100$ %.

Людський фактор впливає також на достовірність, своєчасність та повноту обробки інформації, яку вводять та зберігають у базах даних інформаційної системи. При тривалому вводі даних, в процесі втоми, людина починає робити помилки при вводі, пропускати дані, не вкладається в регламентований час.

Врахування такої характеристики, як здатність до втоми, оцінюється наступним чином. При роботі в сприятливих умовах, середнє напрацювання в останні години зменшується на 6-7% за кожну годину продовження робочого дня більше 6 годин. Тобто, за сьому годину, продуктивність складає 94%, за восьму – 88%, за дев'яту – 81% і т.д. [3]

Ступінь впливу людського фактору на достовірність даних, які вводяться в інформаційну систему при монотонному виконанні операції вводу, можна оцінити, використовуючи значення, які приведені в Таблиці 1.

Таблиця 1

Вплив людського фактору на достовірність вводу інформації.

	Години роботи					
	1-а – 6-а	**7-а**	**8-а**	**9-а**	**10-а**	**11-а**
Продуктивність (% від норми)	100	94	88	81	74	67
Відсоток безпомилковості	0,96	0,9	0,85	0,78	0,71	0,64
Реальний час операції, враховуючи повторні роботи (годин)	6,25	1,11	1,18	1,28	1,4	1,56
Достовірність результатів вводу (відсоток помилок, враховуючи логічні перевірки і повторного вводу)	0,999	0,996	0,994	0,991	0,988	0,985
Верхня границя достовірності	0,9995	0,998	0,997	0,995	0,993	0,991
Нижня границя достовірності	0,997	0,993	0,991	0,987	0,983	0,979

Отже, в таблиці чітко показано, що продуктивність людини суттєво знижується після шостої години роботи. Відповідно негативно впливає на виробництво та захист інформації. Також, зібрані дані в таблиці

підтверджують вище написане. Людський фактор важлива складова у кібербезпеці, ІБ та КСЗІ і її побудові.

Також, одним із важливих питань в даній проблемі є питання «кваліфікації» співробітника, який обслуговує інформаційну систему. Працівник з низькою кваліфікацією та новачки повинні обов'язково проходити етапи навчання і тренування роботи із системою, яка в свою чергу повинна бути відмінно документована.

4. Методологічний підхід до визначення впливу людського фактору на працездатність інформаційної системи

Людина, безумовно впливає на показники надійності та ефективності (повноти, достовірності, своєчасності обробки інформації) ІС в цілому та її окремих підсистем і задач. Методологія оцінки впливу людського фактору на роботу ІС враховує впливи помилок людини на надійність КСЗІ, а також психологічні особливості людини, як ланки даної системи. Вплив людського фактору, а саме операторів, обслуговуючого персоналу сервісних центрів тощо. На роботу інформаційної системи може впливати кількісно визначений ступінь впливу помилок персоналу на безпеку і продуктивність інформаційної системи. Багато процесів в системах, за участі людини, містять потенційні можливості для помилок персоналу, особливо в тих випадках, коли час, що є в розпорядженні оператора для прийняття рішень, обмежений. При цьому ймовірність того, що проблеми будуть розвиватися негативним чином, часто низька. Часом дії персоналу обмежують можливість запобігання початковій несправності, що в подальшому переростає в аварійну ситуацію.

Проте, необхідно ідентифікувати різноманітні типи помилкових дій:

а) помилка через неуважність, помилку, що вилився в невиконанні необхідної дії інформаційної системи;

б) помилка невідповідності, яка може передбачати: становище, коли необхідні дії не виконується належним чином (наприклад, не виконання регламенту адміністрування бази даних);

- дія, що виконується занадто великим або занадто малим зусиллям, або без необхідної точності (наприклад, неточності при заповненні форм введення, помилки неточного введення даних і т.д.);
- дія, що виконується в невідповідний для нього час (наприклад, несвоєчасне введення інформації, затримка обробки інформації і т.д.);
- дія, що виконується з порушенням черговості виконання (наприклад, підготовка підсумкового аналітичного звіту при незавершеному процесі обробки даних);

в) зайва дія, що виконується замість необхідної дії або на додаток до нього (наприклад, повторні введення одних і тих же відомостей, що може привести до розбіжностей у відомостях або появою дублюючих даних).

Ступінь впливу людського фактору на надійність системи можна оцінити за ймовірністю появи помилок у процесі ручного введення даних. Помилка оператора завжди пов'язана з неправильною інтерпретацією надісланих і проаналізованих ним даних. Вважається, що для складних технічних приладів та складних комп'ютерних завдань ймовірність помилки може досягати 15%, для простих технічних пристроїв і нескладних комп'ютерних завдань ймовірність помилки становить від 1% до 5%. Безпомилковість дій оператора залежить від багатьох факторів[2]:

- дефіцит часу (частота здійснення помилок при обробці інформації є логарифмічною функцією швидкості надходження інформації);

- перевантаження інформацією (кількість помилок зростає при перевантаженні, зокрема, при збільшенні числа джерел інформації);
- ступінь підготовки (більш підготовлені фахівці здійснюють в середньому менше помилок);
- психологічні особливості людини (крім того, робота, виконувана з інтересом, як правило, менш хибна);
- «сенсорний голод» (збільшення частоти помилок при тривалому виконанні монотонної роботи).

Важливу роль в питанні зменшення кількості помилок грає ступінь підготовленості оператора. Вважається, що в процесі навчання частота виникнення помилок має тенденцію до зменшення, причому цю залежність можна апроксимувати формулою:

$$q = q_c + (q_0 - q_c) * e^{(-\frac{n}{N})}$$, де

- q – частота помилок після навчання;
- q_0 – початкове значення частоти помилок (до навчання);
- q_c – усталене стаціонарне значення частоти помилок (для навчених операторів);
- n – накопичена сума операцій введення, виконаних оператором в попередніх циклах навчання (роботи);
- N – «Постійне навчання», що характеризує тривалість навчання оператора.

При n = N, різниця (q0> - qc) зменшується на 63%. Вважається, що значення qc досягається через 4 - 5 N. При цьому якщо позначити за n1 - кількість вводів інформації, при якому виконується q = qc, то:

$$N = -\frac{\lg e}{\lg(q_0 - q_c)} n$$

Отримане значення N визначає необхідну кількість вводів інформації, що становить один цикл навчання (тренування) роботи з інформаційною системою.

За експериментальними даними, одержаними під час відпрацювання операторами зорових сигналів, обчислені наступні значення перерахованих вище параметрів:

- q0 = 0,27 (новачки, які не вміють працювати з інформаційною системою),
- q_c = 0,018 (оператори, які пройшли 4 і більше тренувань)

У припущенні, що зовсім навчених роботі з інформаційною системою операторів, як правило, немає, відсоток помилок q0 = 0,27 не досягається. За максимальне значення може бути прийнятий показник q01 = 0,15.

Тоді коефіцієнт обліку помилок етапу ручного введення можна обчислити за формулою:

$$\mathrm{P_{рв}} = 1 - q = \frac{\sum_{i=1}^{N_{\text{ну}}} 1 - q_i}{N_{\text{ну}}}$$

, де $P_{рв}$ – ймовірність безпомилковості етапу ручного введення оцінюється для кожного ручного процесу окремо; якщо процеси послідовні, коефіцієнти перемножуються, тобто

$$\mathrm{P_{рв}} = \prod_{i=1}^{M} P_{\text{рв}\,i}$$

, де

- M – кількість послідовних процесів ручного введення,
- $N_{н.у.}$– кількість операторів, за якими зібрана статистика про помилки.

Імовірність появи помилки оператора істотно залежить від швидкості надходження інформації. Ймовірність прояву помилки в залежності від

швидкості надходження інформації V (біт / с) можна представити наступною формулою:

$$q_{рв} = 9,7\ 10^{-4}\ V^{1,77}$$

Важливість завдання оцінки впливу людського фактору, може бути проілюстрована хоча б аварійною ситуацією, що мала місце при експлуатації однієї з великих розподілених інформаційних систем в серпні 2005 року, коли помилкові дії оператора призвели до знищення робочої бази даних, а її відновлення зайняло декілька днів. Ситуація була викликана тим, що оператор в порушення інструкції не створював щотижня резервні копії бази даних, мотивуючи це тим, що операція резервного копіювання вимагає тривалого часу. Такого роду аварії (авторам відомі більше двох десятків подібних ситуацій, що виникали в різний час на реальних великих інформаційних систем) є застереженням від тих оцінок ризику, які концентрують увагу виключно на технічних і програмних засобах інформаційних систем і ігнорують помилки персоналу.

Крім визначення можливості виникнення катастрофічних ситуацій внаслідок впливу людського фактору, корисно визначити помилки, що знижують продуктивність, ефективність вирішення поставленого завдання в інформаційній системі.

Методологічний підхід до визначення впливу людського фактору може включати в себе наступні етапи:

1. Аналіз завдання або підсистеми інформаційної системи;
2. Визначення ступеня завантаженості задач і підсистем «ручними» операціями, що здійснюються персоналом;
3. Визначення можливих помилок персоналу;
4. Кількісне або якісне визначення впливу людського фактору на надійність інформаційної системи і достовірність зберігається в ній;

5. Рекомендації по автоматизації завдань інформаційної системи, спрямовані на зниження впливу людського фактору.

На стадіях обстеження «ручних» операцій і виявлення помилок персоналу ідентифікуються і описуються можливі помилкові дії при виконанні завдання. Визначення помилок персоналу може включати виявлення можливих наслідків і причин помилкових дій, а також пропозицію заходів щодо зниження ймовірності цієї помилки, вдосконалення перспектив для виправлення і / або зменшення наслідків помилкових дій. Результати обстеження «ручних» операцій та рекомендації по їх автоматизації, таким чином, забезпечують цінний внесок в управління ризиками в інформаційних системах навіть в разі, якщо не проводиться ніяка кількісна оцінка впливу людського фактору.

Кількісна оцінка впливу людського фактору на надійність і ефективність інформаційної системи має на меті оцінити ймовірності правильного виконання того чи іншого завдання (P) або ймовірності помилкових дій (Q = 1 - P). Можна також передбачати кроки по оцінці ймовірності або частоти певних послідовностей небажаних подій або небажаних наслідків.

Імовірність правильного виконання оператором свого завдання $P_{рв}$ під час виконання ручної операції з обов'язковою перевіркою в залежності від ступеня підготовленості до роботи з інформаційною системою, становить $0,985 <= P_{рв} <= 0,999$ чи в середньому $P_{рв} = 0,995$

Іншими словами, ймовірність безпомилкового виконання ручної операції людиною ($P_{рв}$) буде знаходитися в діапазоні від 0,985 до 0,999 в залежності від кваліфікації, ступеня втоми, ступеня перевантаженості роботою тощо. Вірогідність здійснення помилки ($Q_{рв}$) буде знаходитися в діапазоні від 0,001 до 0,015 (від 0,1% до 1,5% даних, що вводяться). Більш повну залежність $P_{рв}$ від тривалості виконання монотонної роботи можна подивитися в Таблиці 1.

Для ручних операцій введення даних, які виконуються в складному завданні (велика інформаційна навантаження, складний інтерфейс) без контрольної перевірки, значення $P_{рв}$ матимуть діапазон від 0,85 до 0,982. Іншими словами, ймовірність здійснення помилки ($Q_{рв}$) буде знаходитися в діапазоні від 0,018 до 0,15 (від 1,8% до 15%). У простих завданнях $Q_{рв}$ буде перебувати в діапазоні від 0,01 до 0,05 (від 1% до 5%).

В цілому ж для інформаційної системи і її основних частин важливо виявити ступінь залежності її окремих завдань і підсистем від операцій, що виконуються «вручну», визначити, чи можна автоматизувати ручні операції. Для операцій, які з якихось причин автоматизувати важко (принципова неможливість, велико вартісні роботи по автоматизації), необхідно розробити організаційні або інші заходи, що знижують можливість впливу індивідуальних властивостей людини на роботу інформаційної системи (документування, навчання, розробка коротких пам'яток та інструкцій) .

Основною можливістю знизити вплив людського фактору на систему, є автоматизація операцій в системі, максимальне скорочення обов'язкових операцій, що виконуються людиною.

Безумовно, є операції, які автоматизувати неможливо або мають велику вартість. Але в цьому випадку, як правило, можна вжити організаційних та інших заходів для зниження впливу людського фактору.

У разі відсутності даних для точного визначення рівня автоматизації можна використовувати якісну оцінку ступеня завантаженості завдання «ручними» операціями: «дуже висока», «висока», «середня», «низька», а також оцінку добре це чи погано для даного завдання або підсистеми. Пропоновані оцінки характеризуються оцінкою відсотка виконуваних в завданні ручних операцій, а також трудомісткістю введення даних, складністю роботи з призначеним для користувача інтерфейсом, темпом виконання роботи.

Застосування математичного апарату оцінки достовірності даних в залежності від помилок ручного введення, дозволяє скласти таблицю залежності помилок ручного введення від ступеня завантаженості завдання «ручними» операціями (див. Таблиця 2). Імовірність введення помилкових відомостей лежить в зазначеному діапазоні і залежить від кваліфікації оператора, ступеня втоми і швидкості введення інформації.

У таблиці, наведеній нижче, показана оцінка можливого помилкового введення даних, в залежності від зовнішніх умов.

Таблиця 2

Приблизний відсоток відомостей, що містять помилки в залежності від ступеня завантаженості завдання ручними операціями

	Оцінка відсотка помилок введення даних $Q_{рв}$ *	
Ступінь завантаженості завдання ручними операціями	**Ручна операція виконана з перевіркою**	**Ручна операція виконана без перевірки**
Низька	0,0001 – 0,003 (0,01 – 0,3 %)	0,01 – 0,05 (1 – 5 %)
Середня	0,001 – 0,010 (0,1 – 1,0 %)	0,02 – 0,10 (2 – 10 %)
Висока	0,001 – 0,015 (0,1 – 1,5 %)	0,02 – 0,12 (2 – 12 %)
Дуже висока	0,003 – 0,022 (0,3 – 2,2 %)	0,05 – 0,15 (5 – 15 %)

У свою чергу ступінь завантаженості завдання (підсистеми) ручними операціями пропонується оцінити в такий спосіб (див. Таблиця 3). Чарунки таблиці заповнюються за наступним принципом: в залежності від оцінки, зазначеної в заголовку колонки №3, рядки колонки 3 заповнюються нулем або одиницею. Тоді останній рядок, що містить суму всіх попередніх, характеризує ступінь завантаженості завдання ручними операціями.

Таблиця 3

Оцінка ступеня завантаженості завдання ручними операціями

№	Характеристика	Оцінка: висока – 1, низька – 0
1	Оцінка кількості виконуваних в завданні ручних операцій	0 чи 1
2	Трудомісткість введення даних	0 чи 1
3	Складність роботи з призначеним для користувача інтерфейсом	0 чи 1
4	Темп виконання «ручної» роботи	0 чи 1
5	Разом (ступінь завантаженості):	1 – Низька 2 – Середня 3 – Висока 4 – Дуже висока

Якщо кожну підсистему або завдання системи проаналізувати згідно з вищенаведеним алгоритмом і заповнити для неї Таблицю 3, то можна оцінити вплив людського фактору в рамках конкретного завдання (підсистеми) на достовірність даних, що вводяться (див. Таблиця 2) і на показники надійності системи в цілому.

Використовуючи дані, наведені в Таблиці 1, можна визначити відсоток помилок з урахуванням втоми людини в залежності від часу роботи.

Таким чином, наведений вище методологічний підхід дозволяє проводити оцінку ступеня впливу людського фактору як для інформаційної системи в цілому, так і для її окремих функцій, задач та побудови, використовуючи дані, які легко отримати, не вдаючись до методів статистичного дослідження.

Висновок. У цій статті була зроблена спроба зібрати і чітко визначити людські фактори, що викликають проблеми інформаційної безпеки і представити пропозиції щодо способів їх подолання. Наслідком цього є те, що інформаційна безпека є ключем до зменшення загроз в інформаційній

безпеці та кібербезпеці, які виникають в наслідок неправильних дій персоналу. Організації повинні розвивати і підтримувати культуру, в якій цінують позитивну поведінку в області інформаційної безпеки. Підприємствам, необхідно підтримувати вектор спрямований на контроль кожної людини в організації, задля підвищення загальної безпеки та продуктивності.

Література

1. Бабак В. Д., Козловський В. В., Хорошко В. 0" Чирков Д. В. Підготовка фахівців із захисту інформації в Україні // Захист інформації. - 2001. - № 4.
2. Лэнд П. Менеджмент – искусство управлять. – М.: ИНФРА–М, 1995. – 144 с.
3. Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to takeremedial measures.