УДК 004.056.5

[https://doi.org/10.33296/2707-0654-9\(18\)-09](https://doi.org/10.33296/2707-0654-9(18)-09)

ОБИДЕННОВА ТЕТЯНА

кандидат економічних наук, доцент
доцент кафедри економіки та менеджменту
Українська інженерно-педагогічна академія,
м. Харків, Україна
ORCIDiD: <https://orcid.org/0000-0002-5548-3906>

НЕГІПА ОЛЕКСАНДР

здобувач 3 курсу першого (бакалаврського)
рівня освіти
Українська інженерно-педагогічна академія,
м. Харків, Україна

**ВИМОГИ ДО ВИБОРУ КЕРІВНИКА СИСТЕМИ МЕНЕДЖМЕНТУ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Анотація. У статті розглянуто проблематику формування вимог до вибору керівника системи менеджменту інформаційної безпеки. Авторами зазначається, що протягом багатьох років проблемам управління інформаційною безпекою суб'єктів господарювання не приділялося достатньої уваги – вони ігнорувалися або повністю, або в достатній мірі. Однак, комплексно розглядаючи роботи українських науковців щодо питань управління інформаційною безпекою, авторами статті зроблено висновок, що ситуація щодо управління інформаційною безпекою поступово змінюється. Небезпека стороннього втручання із можливістю зловживання інформацією з обмеженим доступом є підґрунтям забезпечення захисту інформації – заходів і рішень, що зумовлюють повнофункціональну нормовану роботу суб'єктів господарювання в сучасних умовах. Авторами статті робиться акцент на тому, що ефективність функціонування системи інформаційної безпеки повністю залежить від прийнятих управлінських рішень в системі менеджменту інформаційної безпеки сучасних підприємств, якості і результативності яких повністю залежить від її керівника. Для забезпечення процесу вибору кандидатів на посаду керівника системи менеджменту інформаційної безпеки запропоновано розділити сам процес відбору на конкретні етапи та окреслити відповідні вимоги до результатів на кожному з етапів вибору. На першому етапі пропонується проведення тестування кандидатів, однак, авторами статті наголошено, що результати тестування не можуть бути головними при прийнятті рішення про те, чи підходить кандидат на дану вакансію, а являють собою допоміжні засоби для виявлення тих чи інших здібностей. Тому на другому етапі вибору вимог до вибору керівника системи менеджменту

інформаційної безпеки пропонується отримання достовірних даних щодо наявності у кандидата сертифікатів в області інформаційної безпеки і інформаційних технологій. Авторами статті проаналізовано велику кількість вищезазначених сертифікатів, наявність яких у кандидата говорить про прагнення до самовдосконалення та підтримки професійних знань та навичок на високому рівні у відповідності до вимог сьогодення.

Авторами статті нароблено висновок, що адекватні, доцільні і вчасні вимоги до вибору керівника системи менеджменту інформаційної безпеки сприятимуть обранню ефективного управлінця та професіонала в області інформаційної безпеки і інформаційних технологій. Саме такий підхід сьогодні забезпечить суб'єктам господарювання сталий розвиток та конкурентні переваги в умовах турбулентного середовища функціонування.

Ключові слова: інформаційна безпека, система менеджменту інформаційної безпеки, вибір керівника, тестування, сертифікат.

Вступ. Сучасні умови функціонування характеризуються нестабільністю та турбулентністю. Процеси адаптації суб'єктів господарювання до нових умов ведення бізнесу ускладнюються через брак необхідної інформації. Як наслідок – постійні кризові явища, які швидко погіршують функціонування підприємств. У останні роки все більше власників та топ-менеджерів суб'єктів господарювання приділяють увагу інформаційній безпеці. На багатьох підприємствах створюються окремі підрозділи, головна мета яких – сприяти поліпшенню інформаційного забезпечення суб'єктів господарювання через забезпечення інформаційної безпеки. Цифровізація сучасних господарських процесів ставить перед власниками та топ-менеджерами суб'єктів господарювання завдання вибору керівників системи менеджменту інформаційної безпеки, що матимуть відповідні знання та навички і будуть сприяти забезпеченню інформаційної безпеки в ризикових та нестабільних умовах господарювання.

Аналіз останніх досліджень і публікацій. Усе більше науковців приділяє увагу формуванню економічної безпеки суб'єктів господарювання шляхом забезпечення інформаційної безпеки: О. Дзьобань та О. Соснін [1], Л. Чистоклетов [2], С. Северина [3], А. Марущак [4], О. Кісілевич-Чорнойван [5] та інші. Проте, ефективність функціонування системи інформаційної безпеки

повністю залежить від прийнятих управлінських рішень в системі менеджменту інформаційної безпеки сучасних підприємств, якість і результативність яких повністю залежить від її керівника. Тому питання вимог до вибору керівника системи менеджменту інформаційної безпеки є сьогодні досить актуальним.

Формулювання цілей статті. Метою статті є формування вимог до вибору керівника системи менеджменту інформаційної безпеки сучасних суб'єктів господарювання.

Виклад основного матеріалу дослідження. Сьогодні усе більше власників і топ-менеджерів суб'єктів господарювання розуміють необхідність створення підрозділів, що повинні працювати саме з забезпеченням інформаційної безпеки. Метою роботи таких підрозділів є забезпечення безпеки інформаційних ресурсів суб'єктів господарювання через застосування заходів зі збереження основних властивостей інформації – конфіденційності, доступності, цілісності. Ефективність виконання поставлених завдань багато в чому залежить від керівника системи менеджменту інформаційної безпеки (СМІБ), що буде контролювати процес управління інформаційною безпекою [6]. У таких випадках керівництво зазвичай звертається до HR-менеджера і встановлює для останнього завдання пошуку особи на посаду керівника системи менеджменту інформаційної безпеки.

Для забезпечення процесу вибору кандидатів на посаду керівника системи менеджменту інформаційної безпеки важливо розділити сам процес відбору на конкретні етапи та окреслити відповідні вимоги до результатів на кожному з етапів вибору.

На першому етапі важливим є проведення тестування кандидата.

Тестування може проводитися у такий спосіб:

– неявно – під час співбесіди у такій формі, щоб кандидат про тестування не підозрював. При такій формі тестування кандидат може отримати опис гіпотетичної ситуації, яка відбувається з третіми особами і запитання про думки на цю тему. Такий спосіб тестування надасть можливість кандидату проявити

свої комунікативні навички, показати критичне мислення і вміння реагувати інтуїтивно та максимально швидко;

– явно – із заповненням тестової форми, або відповідями на прямі запитання. Така форма надасть можливість кандидату проявити теоретичні знання з питань інформаційної безпеки та особливостей функціонування суб'єкта господарювання.

Професійні тести є найпоширенішим видом тестування і застосовуються найчастіше. Вони дозволяють визначати рівень знань працівника. Загалом, тестування може перевіряти різні навички та вміння, в залежності від вимог керівництва. Проте, необхідно пам'ятати, що правильно підібрані питання тесту або ситуація до розв'язання допоможе отримати від кандидатів необхідні відповіді і надасть можливість перевірити рівень їх теоретичної підготовки і спроможність вирішувати професійні завдання в сфері інформаційної безпеки суб'єктів господарювання.

Разом з ними часто застосовують інтелектуальні тести. Цей вид тестування не має прямого відношення до тієї посади, на яку розглядається кандидат, а ставить метою визначення рівня розумового розвитку. Найпоширенішими серед інтелектуальних тестів є напрацювання Айзенка і Амтхауера.

Для виявлення реакції на невдачу кандидату на посаду керівника СМІБ і визначення способів виходу з ситуацій, що заважають діяльності або задоволенню особистісних потреб часто застосовується методика фрустраційних реакцій Розенцвейга. Іншими тестами, що застосовуються організаціями при відборі кандидатів на посаду керівника СМІБ можуть бути тест Маркерта «В якому Ви настрої»; тест Кеттелла, тест Роршаха, кольоровий тест Люшера тощо.

Тестування є ефективним засобом відбору, тому що результати тестів можна порівняти з нормованими та між собою і, таким чином, виділити найбільш підходящих осіб. Однак треба розуміти, що результати тестування не

можуть бути головними при прийнятті рішення про те, чи підходить кандидат на дану вакансію, а являють собою допоміжні засоби для виявлення тих чи інших здібностей. Окрім цього, часто на підприємствах тестування використовується для визначення можливості кандидатів співіснувати з робітниками, можливості кандидатів в вихідних умовах співпрацювати та керувати.

На другому етапі важливим є отримання достовірних даних щодо наявності у кандидата сертифікатів в області інформаційної безпеки і інформаційних технологій. Існує велика кількість сертифікатів, тому розглянемо найпоширеніші.

Сертифікація CompTIA вважається не найкращою у світі, але є незалежним і признаним в усьому світі типом сертифікації в сфері інформаційної безпеки. Сертифікат «CompTIA Security+» підтверджує компетенцію в наступних областях: безпека мереж і телекомунікацій, відповідність і операційна безпека, загрози та вразливості, безпека додатків, контроль доступу і керування ідентифікацією, криптографія. Дія сертифіката – три роки.

«CompTIA A+» сертифікація – це програма тестування, надана асоціацією CompTIA, що підтверджує компетенцію фахівців з обслуговування комп'ютерної техніки. Кандидат на отримання сертифіката A+ мусить скласти два екзамени. Перший екзамени – це «CompTIA A+ Essentials (220-601)». Другий, більш складний іспит, здається в залежності від типу бажаного сертифіката. На кожному додатковому іспиті оцінюються спеціальні навички в областях «Спеціаліст з інформаційних технологій», «Інженер з віддаленої підтримки», «Спеціаліст з базового технічного обслуговування» [7].

Сертифікат «CompTIA A+ – основи» свідчить про наявність базових навичок, необхідних для установки, компонування, оновлення, налаштування, усунення неполадок, оптимізації, діагностики і обслуговування базового апаратного забезпечення персонального комп'ютера та операційних систем.

Сертифікат «CompTIA A+ – IT-спеціаліст» свідчить, що власник сертифікату є технічним фахівцем з обслуговування на місці експлуатації і може працювати як на мобільних ПК, так і в корпоративних середовищах.

Сертифікат «CompTIA A+ – інженер з віддаленої підтримки» свідчить, що його власник відповідає за надання допомоги клієнтам без фізичного контакту з комп'ютером клієнта. Сертифікат «CompTIA A+ – спеціаліст з базового технічного обслуговування» показує, що його власник мало спілкується з клієнтами і працює переважно в майстерні або лабораторії.

Сертифікація CompTIA вважається найкращою за кількістю сертифікованих фахівців серед сертифікацій початкового рівня і гарантує фундаментальний рівень знань в області інформаційної безпеки [7].

Сертифікація від вендорів – це сертифікати, що видаються відомими компаніями. До них відносяться компанії Microsoft, Cisco, Oracle Academy, IBM тощо. Наприклад, корпорація Microsoft постійно оновлює сертифікаційні іспити при появі нових версій програмних продуктів. Тому для підтримки постійного рівня своєї кваліфікації спеціаліст зобов'язаний вчасно відстежувати появу нових технологій і продуктів і здавати тести з цим оновленням технологій або версіями продуктів. Існують наступні види сертифікації кадрів компанії Microsoft: MCDST – спеціаліст технічної підтримки Microsoft, MCSA – системний адміністратор Microsoft, MCDBA – адміністратор баз даних Microsoft, MCSE – системний інженер Microsoft, MCAD – розробник додатків на основі продуктів Microsoft, MCSA – розробник програмних рішень на основі продуктів Microsoft, MCITP – професіонал з інформаційних технологій Microsoft тощо [7].

Інститут SANS вважається одним з усесвітньо визнаних авторитетів у галузі безпеки. Крім різноманітних курсів, тренінгів, публікацій і досліджень, при SANS створений спеціальний центр аналізу інцидентів GIAC, який поряд з іншою своєю діяльністю пропонує і сертифікацію технічних фахівців з безпеки [7].

GIAC пропонує три рівня підтвердження своєї кваліфікації – GSEc (базовий рівень), GCFW/GCIA/GCIH/GCNT/GCUX і GSE. GIAC виокремлює кілька напрямків розвитку своїх випускників. Сертифікат GCFW характеризує власника як фахівця в роботі з міжмережевими екранами, захистом периметра, VPN і діє чотири роки. Сертифікатом GCIA, терміном дії в чотири роки, володіє фахівець з виявлення атак. Сертифікат GCIH з управління інцидентами необхідно підтверджувати кожні два роки. Сертифікати GCNT і GCUX представляють собою фахівців з безпеки Windows- та Unix-подібних операційних систем. Цей статус необхідно підтверджувати кожні два роки. Зменшення часу на ресертифікацію пов'язано з швидкою зміною ситуації на ринку «хакерських технологій» і необхідністю відповідати всім сучасним тенденціям.

Найвищий ступінь сертифікації GIAC в області інформаційної безпеки – сертифікат GSE можливо отримати лише отримавши базовий статус GSEc і п'ять перерахованих вище сертифікацій – GCFW, GCIA, GCIH, GCNT і GCUX [10]. Цей сертифікат є достатнім для прийняття кандидата на посаду керівника СМІБ в штат працівників, якщо інші критерії претендента задовольняють умовам прийому.

Навчальний центр Мікроінформ і Міжнародний Консорціум з Сертифікації в області Безпеки Інформаційних Систем (ISC)² пропонує дві сертифікації: «Сертифікований професіонал в області безпеки інформаційних систем» – CISSP, що розглядається в усьому світі як «Золотий Стандарт» серед сертифікацій для професіоналів вищого рівня у галузі інформаційної безпеки, і «Сертифікований фахівець-практик з безпеки систем» – SSCP, для фахівців в області комп'ютерної безпеки, що на практиці реалізують політики безпеки.

Звання CISSP дає незалежне і об'єктивне підтвердження професійної майстерності та знання в сфері індустрії інформаційної безпеки. Умовами отримання сертифікації є необхідний практичний досвід – чотири роки роботи в сфері інформаційної безпеки, або три роки плюс ступінь бакалавра,

відповідна підготовка та здача іспиту, заснованого на загальному обсязі знань СВК.

СВК представляє собою збірник кращих методів забезпечення безпеки в десяти областях: системи і методологія контролю доступу, захист розробки додатків і систем, планування безперервності бізнесу та усунення неполадок, криптографія, право, дослідження і етика, захист операцій, фізична безпека, архітектура і моделі безпеки, методи управління безпекою, безпека телекомунікацій і мереж. Окрім екзамену і досвіду роботи, претенденти також підписують кодекс етики (ISC)². Сертифікація підтримується за допомогою тривалого професійного навчання CPE.

Сертифікат SSCP створений спеціально для фахівців-практиків у галузі інформаційної безпеки систем і вимагає досвіду роботи в областях СВК протягом не менш як одного року.

Професіонали, що змогли отримати сертифікат CISSP, протягом трьох років повинні набрати певну кількість балів за рахунок подальшого професійного навчання, підтвердивши таким чином свою активність у цій області. SSCP вимагає досвіду роботи не менше року як мінімум в одній з семи областей знань СВК [7].

Найбільшої популярності серед фахівців в області інформаційної безпеки набули сертифікати міжнародної асоціації ISACA. Існує чотири види сертифікатів ISACA.

Сертифікат CISA характеризує свого власника як аудитора інформаційних систем з досвідом роботи в галузі аудиту інформаційних систем та інформаційної безпеки. Сертифікат CISM представляє сертифікованого менеджера в області інформаційної безпеки. Сертифікація націлена на професіоналів, які займаються розробкою, впровадженням, підтримкою та поліпшенням СМІБ в організаціях. Сертифікат CGEIT свідчить, що його власник є сертифікованим професіоналом в області управління корпоративними інформаційними технологіями і професіоналом в області

управління, консультування, аудиту та підтримки планування функції корпоративних інформаційних технологій. Сертифікат CRISC показує, що його володілець – сертифікований професіонал в області управління ризиками, професіонал, що має досвід в ідентифікації ризиків, їх оцінці, виробленні контрольних заходів та їх моніторингу.

Відповідно до правил асоціації, для підтримки професійної кваліфікації, володарі сертифікатів протягом трьох років з моменту видачі сертифікатів повинні набрати встановлену кількість CPE – тобто встановлену кількість «годин безперервного навчання» [7].

Таким чином, дивлячись на різноманіття сертифікатів, кількість вимог до кандидата на посаду керівника СМІБ та різноманітність їх характеристик, можна зробити висновок, що задача відбору найбільш підходящої особи на посаду керівника СМІБ є багатокритеріальною і потребує вирішення згідно з одним із методів вирішення багатокритеріальних задач.

Висновки. Формування вимог до вибору керівника системи менеджменту інформаційної безпеки є одним з головних питань забезпечення ефективного функціонування суб'єктів господарювання. Адекватні, доцільні і вчасні вимоги сприятимуть обранню ефективного управлінця та професіонала в області інформаційної безпеки і інформаційних технологій. Доцільним є отримання уявлення щодо теоретичної підготовки кандидата на посаду керівника СМІБ, а також наявність у нього одного з сертифікатів в області інформаційної безпеки і інформаційних технологій, що говорить про прагнення до самовдосконалення та підтримки професійних знань та навичок на високому рівні у відповідності до вимог сьогодення. Саме такий підхід до формування вимог до вибору керівника системи менеджменту інформаційної безпеки сьогодні забезпечить суб'єктам господарювання сталий розвиток та конкурентні переваги в умовах турбулентного середовища функціонування.

Використана література

1. Дзьобань О. П. , Соснін О. В. Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною діяльністю *Гуманітарний вісник Запорізької державної інженерної академії*. 2015. Вип. 61. С. 24–34.
2. Чистоклетов Л. Г. Інформаційна безпека підприємства – як складова економічної безпеки: сучасні реалії та загрози. *Наукові записки Львівського університету бізнесу та права*. 2011. Вип. 7. С. 222–227.
3. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки*. 2016. № 1. С. 155–161.
4. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 9295.
5. Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. 2009. № 8. С. 11-18.
6. Обиденнова Т.С., Гусаров О.О., Антипцева О.Ю. Методи прийняття управлінських рішень в умовах розроблення, впровадження та функціонування системи менеджменту інформаційної безпеки. *Проблеми системного підходу в економіці*. 2019. Вип. 2(70). С. 153-157.
7. Центр аудиту інформаційної безпеки. Київ. – 2012. – URL: <http://bezpeka.ladimir.kiev.ua/study.php>.
8. Дуднєва Ю., Лугова І., Котелевець Т. Проблеми кадрової політики сучасного неприбуткового підприємства. *Адаптивне управління: теорія і практика. Серія Економіка*. 2020. 8(16). – URL: <https://amtp.org.ua/index.php/journal2/article/view/294>

References

1. Dzoban O. P. , Sosnin O. V. Informatsiina bezpeka: novi vymiry zahroz, poviazanykh iz informatsiino-komunikatsiinoiu diialnistiu Humanitarnyi visnyk Zaporizkoi derzhavnoi inzhenernoi akademii. 2015. Vyp. 61. S. 24-34.
2. Chystokletov L. H. Informatsiina bezpeka pidpriemstva – yak skladova ekonomichnoi bezpeky: suchasni realii ta zahrozy. Naukovi zapysky Lvivskoho universytetu biznesu ta prava. 2011. Vyp. 7. S. 222-227.
3. Severyna S. V. Informatsiina bezpeka ta metody zakhystu informatsii. Visnyk Zaporizkoho natsionalnoho universytetu. Ekonomichni nauky. 2016. № 1. S. 155-161.
4. Marushchak A. I. Informatsiino-pravovi napriamy doslidzhennia problem informatsiinoi bezpeky. Derzhavna bezpeka Ukrainy. 2011. № 21. S. 9295.

5. Kisilevych-Chornoivan O. M. Informatsiina bezpeka ta mizhnarodna informatsiina bezpeka: problema vyznachennia poniat. Yurysprudentsiia: teoriia i praktyka. 2009. № 8. S. 11-18.

6. Obydiennova T.S., Husarov O.O., Antyptseva O.Iu. Metody pryiniattia upravlinskykh rishen v umovakh rozroblennia, vprovadzhennia ta funktsionuvannia systemy menedzhmentu informatsiinoi bezpeky. Problemy systemnoho pidkhodu v ekonomitsi. 2019. Vyp. 2(70). S. 153-157.

7. Tsentru audytu informatsiinoi bezpeky. Kyiv. – 2012. – URL: <http://bezpeka.ladimir.kiev.ua/study.php>.

8. Dudnieva Yu., Luhova I., Kotelevets T. Problemy kadrovoi polityky suchasnoho neprybutkovoho pidpriiemstva. Adaptivne upravlinnia: teoriia i praktyka. Seriia Ekonomika. 2020. 8(16). – URL: <https://amtp.org.ua/index.php/journal2/article/view/294>

ОБЫДЕННОВА ТАТЬЯНА

кандидат экономических наук, доцент
доцент кафедры экономики и менеджмента
Украинская инженерно-педагогическая академия,
г. Харьков, Украина

НЕГИПА АЛЕКСАНДР

соискатель 3 курса первого (бакалаврского) уровня образования
Украинская инженерно-педагогическая академия,
г. Харьков, Украина

ТРЕБОВАНИЯ К ВЫБОРУ РУКОВОДИТЕЛЯ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В статье рассмотрена проблематика формирования требований к выбору руководителя системы менеджмента информационной безопасности. Авторами отмечается, что в течение многих лет проблемам управления информационной безопасностью субъектов хозяйствования не уделялось достаточного внимания – они игнорировались полностью или в достаточной мере. Однако, комплексно рассматривая работы украинских ученых в вопросах управления информационной безопасностью, авторами статьи сделан вывод, что ситуация по управлению информационной безопасностью постепенно меняется. Опасность постороннего вмешательства с возможностью злоупотребления информацией с ограниченным доступом является основой обеспечения защиты информации – мер и решений, обуславливающие полнофункциональную нормированную работу субъектов хозяйствования в современных условиях. Авторами статьи делается акцент на том, что эффективность функционирования системы информационной

безопасности полностью зависит от принятых управленческих решений в системе менеджмента информационной безопасности современных предприятий, качество и результативность которых полностью зависит от ее руководителя. Для обеспечения процесса выбора кандидатов на должность руководителя системы менеджмента информационной безопасности предложено разделить сам процесс отбора на конкретные этапы и определить соответствующие требования к результатам на каждом этапе выбора. На первом этапе предлагается проведение тестирования кандидатов, однако, авторами статьи отмечено, что результаты тестирования не могут быть главными при принятии решения о том, подходит ли кандидат на данную вакансию, а представляют собой вспомогательные средства для выявления тех или иных способностей. Поэтому на втором этапе выбора требований к выбору руководителя системы менеджмента информационной безопасности предлагается получение достоверных данных о наличии у кандидата сертификатов в области информационной безопасности и информационных технологий. Авторами статьи проанализировано большое количество вышеупомянутых сертификатов, наличие которых у кандидата говорит о стремлении к самосовершенствованию и поддержки профессиональных знаний и навыков на высоком уровне в соответствии с требованиями современности.

Авторами статьи наделян вывод, что адекватные, целесообразные и своевременные требования к выбору руководителя системы менеджмента информационной безопасности будут способствовать выбору эффективного управленца и специалиста в области информационной безопасности и информационных технологий. Именно такой подход сегодня обеспечит субъектам хозяйствования устойчивое развитие и конкурентные преимущества в условиях турбулентной среды функционирования.

Ключевые слова: информационная безопасность, система менеджмента информационной безопасности, выбор руководителя, тестирование, сертификат.

OBYDIENNOVA TETIANA

PhD of Economics, Associate Professor,
Associate Professor of Economics and Management
Ukrainian Engineering and Pedagogics Academy, Kharkiv, Ukraine

NEHIPA OLEKSANDR

3rd year student of the first (bachelor's) level of education
Ukrainian Engineering and Pedagogical Academy, Kharkiv, Ukraine

REQUIREMENTS FOR THE SELECTION OF THE HEAD OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

Abstract. The article considers the issue of forming requirements for the selection of the head of the information security management system. The authors

note that for many years, the problems of information security management of business entities have not been given enough attention - they have been ignored either completely or sufficiently. However, considering the work of Ukrainian scientists on information security management, the authors of the article concluded that the situation with information security management is gradually changing. The danger of outside interference with the possibility of misuse of information with limited access is the basis for ensuring the protection of information – measures and solutions that lead to full-fledged standardized work of business entities in modern conditions. The authors of the article emphasize that the effectiveness of the information security system depends entirely on management decisions in the information security management system of modern enterprises, the quality and effectiveness of which depends entirely on its head. To ensure the process of selecting candidates for the position of head of the information security management system, it is proposed to divide the selection process into specific stages and outline the relevant requirements for the results at each stage of selection. At the first stage, it is proposed to test candidates, however, the authors emphasize that the test results can not be the main factor in deciding whether a candidate is suitable for this vacancy, but are aids to identify certain abilities. Therefore, at the second stage of the selection of requirements for the selection of the head of the information security management system, it is proposed to obtain reliable data on the availability of the candidate's certificates in the field of information security and information technology. The authors of the article analyzed a large number of the above certificates, the presence of which the candidate indicates a desire for self-improvement and maintenance of professional knowledge and skills at a high level in accordance with today's requirements.

The authors of the article concluded that adequate, appropriate and timely requirements for the selection of the head of the information security management system will facilitate the selection of an effective manager and professional in the field of information security and information technology. This is the approach that will provide businesses today with sustainable development and competitive advantage in a turbulent environment.

Key words: information security, information security management system, selection of the head, testing, certificate.