

Додаток
до наказу Національної комісії з цінних
паперів та фондового ринку

ЗАТВЕРДЖУЮ
Керівник офісу Національної комісії
з цінних паперів та фондового ринку
Костянтин МОСЕНЦЕВ
(підпис) (власне ім'я та прізвище)

«__» _____ 20__ р.

Профіль посади
начальника відділу кібербезпеки та захисту інформації
Національної комісії з цінних паперів та фондового ринку

І. Найменування посади	
Найменування державного органу	Національна комісія з цінних паперів та фондового ринку
Найменування самостійного структурного підрозділу (за наявності)	Відділ кібербезпеки та захисту інформації
Найменування структурного підрозділу	
Найменування посади	Начальник відділу кібербезпеки та захисту інформації
Основні посадові обов'язки	Забезпечення інформаційної безпеки/кібербезпеки та захисту інформації щодо інформаційних ресурсів у розпорядженні Комісії відповідно до нормативних та внутрішніх вимог з урахуванням світового досвіду, поширених стандартів, практик і технологій: формування пропозицій щодо політики інформаційної безпеки в Комісії; побудова системи управління інформаційною безпекою в Комісії;



ДОКУМЕНТ СЕД АСКОД
Сертифікат 6FA97849F1B2570D0400000048B2010044280A00
Підписувач Мосенцев Костянтин Вікторович
Дійсний з 12/16/2025 10:48:16 AM по 12/16/2026 10:48:16 AM

Національна комісія з цінних паперів та фондового ринку

№ 18/20/4985/C02 від 07.08.2026

	проєктування, організація, впровадження та контролю заходів щодо забезпечення інформаційної безпеки в Комісії; забезпечення функціонування резервного інформаційно-комунікаційного майданчика; проведення аналітичної оцінки поточного стану безпеки інформації в АС та в Комісії загалом, складання звіту за результатами проведення оцінки; управління інформаційними ризиками. Забезпечення дотримання нормативних вимог щодо захисту інформації, що передбачає: розроблення проєктів поточних і перспективних планів щодо побудови системи захисту інформації; встановлення вимог до організації роботи, пов'язаної із захистом персональних даних відповідно до Закону України «Про захист персональних даних»; організацію та координацію робіт із проєктування та розробки систем захисту інформації (СЗІ) та/або комплексної системи захисту інформації в Комісії (КСЗІ), безпосередню участь у проєктних роботах із створення СЗІ та/або КСЗІ; забезпечення застосування електронного цифрового підпису (печатки) в Комісії та контролю за дотриманням вимог його використання підписувачами; розроблення та коригування моделей загроз і моделей захисту інформації в автоматизованих системах Комісії, політик безпеки інформації, визначення заходів щодо їх реалізації; розроблення регламентів допуску працівників Комісії та сторонніх осіб до окремих видів інформації, категоризованих
--	--

	приміщень та носіїв інформації; взаємодію з органами державної влади з питань захисту інформації. Забезпечення питань захисту критичної інфраструктури сектору «ринки капіталу та організовані товарні ринки». Забезпечення побудови систем захисту інформації та/або КСЗІ для автоматизованих систем Комісії. Планування та забезпечення здійснення заходів щодо реалізації Стратегії кібербезпеки України. Участь у взаємодії основних суб'єктів національної системи кібербезпеки в частині спільного виконання завдань кіберзахисту. Розроблення та виконання плану кіберзахисту. Підвищення рівня обізнаності у сфері кібербезпеки шляхом проведення тематичних навчань, семінарів, нарад та/або заходів за участю працівників Комісії. Забезпечення взаємодії з CERT-мережею (CERT-UA). Участь у розробці проєктів актів Комісії з питань, що належать до компетенції відділу.
II. Кваліфікаційні вимоги	
Освіта	Вища освіта за освітнім ступенем не нижче магістра за спеціальностями галузі знань F «Інформаційні технології».
Стаж роботи	Досвід роботи на керівних посадах підприємств, об'єднань, установ та організацій незалежно від форми власності не менше трьох років за професійним спрямуванням.
Володіння державною мовою	Вільне володіння державною мовою.
Володіння іноземними мовами	Володіння англійською мовою на рівні, достатньому для опрацювання професійної, нормативної та технічної документації у сфері інформаційної та кібербезпеки (ISO/IEC 27001, NIST CSF – стандарти, які прописані англійською мовою).
Знання законодавства відповідно до	Конституція України;

посадових обов'язків	Закон України «Про державне регулювання ринків капіталу та організованих товарних ринків»; Закон України «Про ринки капіталу та організовані товарні ринки»; Закон України «Про запобігання корупції»; Закон України «Про основні засади забезпечення кібербезпеки України»; Закон України «Про захист інформації в інформаційно-комунікаційних системах»; Закон України «Про захист персональних даних»; Закон України «Про державну таємницю»; Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»; Постанова Кабінету Міністрів України від 18 червня 2025 р. № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», зокрема Порядок авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем.
Професійні знання	розроблення політик безпеки, нормативно-технічних і розпорядчих документів; організація криптографічного та технічного захисту інформації; моделювання загроз, виявлення ймовірних каналів витоку інформації; реагування на інциденти (Incident Response): виявлення, аналіз, локалізація, нейтралізація; робота із SIEM/XDR-системами — на рівні контролю та читання звітів; моніторинг інформаційної безпеки, аналіз логів (Linux/Windows); загальне розуміння адміністрування інформаційних систем; знання міжнародних стандартів ISO/IEC 27001, NIST CSF;

	підготовка проєктів наказів та організаційно-розпорядчих документів; організація професійної підготовки персоналу та користувачів з питань захисту інформації; побудова системи управління інформаційною безпекою (СУІБ) за ризик-орієнтованою моделлю; застосування базових профілів безпеки залежно від типу інформації (відкрита / з обмеженим доступом) та призначення системи; проходження процедури авторизації з безпеки ІКС за Порядком КМУ № 712 від 18.06.2025; оцінювання дотримання вимог цільового профілю безпеки; знання перехідних положень від КСЗІ до нової моделі авторизації; розуміння мережевих протоколів (TCP/IP, DNS, DHCP, VPN, HTTP/S) та принципів маршрутизації; принципи розмежування мережі, категорії апаратних (технічних) засобів захисту інформації.
Вимоги до компетентності	Управлінські компетентності: здатність організовувати роботу відділу та ефективно розподіляти завдання між працівниками; здатність визначати пріоритети, планувати роботу та забезпечувати досягнення визначених результатів; здатність приймати обґрунтовані управлінські рішення в умовах ризику та невизначеності; здатність ефективно взаємодіяти з керівництвом Комісії, структурними підрозділами, державними органами та іншими суб'єктами у сфері кібербезпеки. Аналітичні компетентності: системне та стратегічне мислення; здатність аналізувати кіберризики, загрози та вразливості; здатність працювати з великими обсягами інформації та приймати рішення на основі її аналізу.

	Професійні компетентності: здатність застосовувати законодавство та професійні стандарти у сфері інформаційної та кібербезпеки; здатність організовувати впровадження сучасних підходів і технологій кіберзахисту; здатність організовувати реагування на кіберінциденти та координацію відповідних заходів; здатність забезпечувати постійне вдосконалення системи інформаційної та кібербезпеки. Особистісні компетентності: відповідальність та доброчесність; орієнтація на результат; здатність швидко опановувати нові знання та технології; здатність працювати в умовах підвищеного навантаження та невизначеності; комунікабельність та здатність до конструктивної взаємодії; уважність до деталей. Спеціальні вимоги: наявність або готовність до оформлення допуску до державної таємниці у випадках, визначених законодавством.
III. Інші відомості	
Умови оплати праці	Посадовий оклад – 49 265 грн.
Інформація про строковість чи безстроковість призначення на посаду	Строково, на умовах трудового договору
Перелік інформації та документів, необхідних для участі у відборі	1. Заява про участь у відборі згідно з додатком 3 до Умов найму працівників Національної комісії з цінних паперів та фондового ринку затверджених рішенням Національної комісії з цінних паперів та фондового ринку 10 грудня 2024 року № 15/21/1552/К03; 2. Резюме, у якому зазначається: прізвище, власне ім'я, по батькові (за наявності);

	дата і місце народження; адреса за місцем фактичного проживання (вулиця, номери будинку та квартири (за наявності), населений пункт (місто, селище, село), район, область, поштовий індекс); адреса зареєстрованого/задекларованого місця проживання (вулиця, номери будинку та квартири (за наявності), населений пункт (місто, селище, село), район, область, поштовий індекс); адреса електронної пошти; контактний номер телефону; реквізити документа, що посвідчує особу та підтверджує громадянство України; відомості про отримання відповідного ступеня вищої освіти (назва закладу освіти, серія, номер, дата видачі документа про освіту), інші відомості про отриману освіту; трудова діяльність із зазначенням дати прийому та звільнення; інші знання, вміння, навички тощо. Особа, яка бажає взяти участь у відборі, може подавати додаткову інформацію стосовно своєї освіти, досвіду роботи, професійного рівня і репутації (характеристики, рекомендації, наукові публікації тощо), мотиваційний лист. На документи (електронні копії документів), що подаються шляхом надсилання на електронну пошту Комісії з відбору, накладається кваліфікований електронний підпис кандидата.
Строк подання документів	до 16 год. 45 хв. 14 серпня 2026 року
Адреса, на яку надсилаються (за якою приймаються) документи	hr@nssmc.gov.ua
Номер телефону, за яким надається інформація з питань проведення відбору	(044) 254-24-94
Місце проведення відбору	вул. Князів Острозьких, 8, корпус 30,

	м. Київ, 01010
--	----------------
