|  |
| --- |
| **ЗАТВЕРДЖЕНО**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Директор з інформаційної безпеки Департаменту інформаційної безпеки Є.Є. Балютов  «24» жовтня 2024 р. |
|  |

**ПОСАДОВА ІНСТРУКЦІЯ**

|  |  |
| --- | --- |
| **Посада** | Менеджер з питань автоматизації процесу керування доступами |
| **Структурний підрозділ /Дирекція/Відділення** | Управління менеджменту інформаційної безпеки Департаменту інформаційної безпеки |
| **Підпорядкування** | Начальник управління менеджменту інформаційної безпеки Департаменту інформаційної безпеки |
| **Заміщення** | Під час відсутності менеджера з питань автоматизації процесу керування доступами відповідно до штатного розпису заміщує інший працівник управління ІТ безпеки, або працівник управління менеджменту інформаційної безпеки за цією посадою у встановленому в Банку порядку. |
| Менеджер з питань автоматизації процесу керування доступами відповідно до штатного розпису заміщує іншого працівника управління ІТ безпеки, або працівника управління менеджменту інформаційної безпеки за цією посадою під час його відсутності у встановленому в Банку порядку. |
| **Основні обов’язки за посадою** | 1. Супроводження процесів з автоматизації керування доступом користувачів до інформаційних ресурсів Банку.  2. Організація роботи та забезпечення контролю за належним виконанням працівниками напрямку функції з впровадження, забезпечення та подальшого вдосконалення роботи системи автоматизованого керування доступом користувачів до інформаційних ресурсів Банку.  3. Організація роботи та забезпечення контролю за належним виконанням працівниками напрямку функції з інтеграції інформаційних ресурсів з системою автоматизованого керування доступом.  4. Організація роботи та забезпечення контролю за належним виконанням працівниками напрямку функції з супроводження процесу з автоматизованого керування рівнем доступу (надання / модифікація / позбавлення) користувачів до інформаційних ресурсів Банку.  5. Організація роботи та забезпечення контролю за належним виконанням працівниками напрямку функції з супроводження процесу з автоматизованого керування даними автентифікації користувачів до інформаційних систем.  6. Організація роботи та забезпечення контролю за належним виконанням працівниками напрямку функції з супроводження процесу з автоматизованого керування паролями користувачів (генерація, визначення первинного / тимчасового, скидання і вирішення проблемних питань пов’язаних з паролями користувачів) та забезпечення передачі паролів до інформаційних ресурсів Банку.  7. Організація роботи та забезпечення контролю за належним виконанням працівниками напрямку функції з опрацювання запитів бізнес-підрозділів Банку стосовно доступу до інформаційних ресурсів Банку, аналіз та оперативне вирішення проблем, які пов’язані з керуванням доступу користувачів.  8. Виконання вимог чинного законодавства України (далі – чинне законодавство), нормативно-правових актів НБУ, Статуту АТ “Райффайзен Банк”, Колективного договору, нормативних документів Банку, рішень Правління та інших органів Банку, наказів, розпоряджень Банку в межах Положення про Управління ІТ безпеки та цієї Посадової інструкції.  9. Дотримання вимог інформаційної безпеки, зберігання та нерозголошення інформації, яка становить банківську таємницю та іншу конфіденційну інформацію Банку, яка стане відомою під час роботи в Банку та після припинення (розірвання) трудових відносин з Банком без обмеження строком.  10. Підвищення своєї кваліфікації шляхом участі у семінарах/тренінгах у відповідності до планів Банку, самостійного навчання.  11. Дотримання вимог Політики комплаєнсу АТ «Райффайзен Банк», виконання своїх посадових обов’язків виключно в інтересах Банку та його клієнтів, недопущення випадків, що можуть стати причиною конфлікту інтересів та завдати матеріальної шкоди та/або негативно вплинути на репутацію Банку.  12. Виконання вимог з техніки безпеки, правил та норм охорони праці.  13. Виконання інших обов’язків та здійснення іншої діяльності згідно з Положенням про управління менеджменту інформаційної безпеки та Положенням про управління ІТ безпеки Департаменту інформаційної безпеки, завданнями керівництва, у тому числі розпорядженнями Директора з інформаційної безпеки Департаменту інформаційної безпеки. |
| **Відповідальність** | За невиконання / неналежне виконання обов’язків за посадою, порушення вимог законодавства та/або нормативних/розпорядчих документів Банку під час виконання роботи, до працівника можуть бути застосовані дисциплінарні стягнення, а також інші заходи впливу та відповідальність, передбачені законодавством та нормативними документами Банку. |
| **Вимоги** | **Освіта:**  вища освіта за напрямом підготовки інформаційна безпека та захист інформації. |
| **Досвід роботи:**  за фахом та на відповідних посадах в банківській сфері або близької до неї діяльності не менш 2 років. |
| **Фахові знання та ключові навички:** Знати нормативні документи Банку, нормативно-правові акти НБУ, директиви Групи та галузеві міжнародні стандарти, які регламентують питання інформаційної безпеки та вміти вірно застосовувати їх при виконанні цієї посадової інструкції. Мати навички роботи з основними операційними системами та спеціальним програмним забезпеченням. Знати перелік інформації, що становить банківську чи комерційну таємниці, або носить конфіденційний характер. |
| **Додаткові компетенції:**  Постійно підвищувати свій професійний рівень. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **З посадовою інструкцією ознайомлений(на)** | |  | |  | |
| “24” жовтня 2024 р**.** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | | **М.М. Чернов** | |