29. Відділ інформаційної безпеки

1. Відділ відповідно до покладених на нього завдань:

1) забезпечує інформаційну безпеку Фонду;

2) виконує обов’язки адміністратора інформаційної безпеки засобів захисту інформації для автоматизованого робочого місця «АРМ-НБУ-інф.» та системи «Клієнт–банк» Національного банку України у Фонді, а також у банку при здійсненні повноважень під час здійснення ліквідації банку Фондом безпосередньо;

3) забезпечує отримання для Фонду, а також у банку при здійсненні повноважень під час здійснення ліквідації банку Фондом безпосередньо, засобів криптозахисту та їх заміну в Національному банку України та здійснює тестування програмного модуля генерації ключів криптографічного захисту Національного банку України;

4) виконує роботи з програмування та забезпечення функціонування систем відеоспостереження, охоронної сигналізації та контролю доступу до будівлі та приміщень Фонду, забезпечує виготовлення та видачу персональних посвідчень працівників Фонду;

5) збирає інформацію щодо дотримання працівниками та відвідувачами встановленого режиму доступу в приміщення Фонду та правил роботи з персональними комп’ютерами;

6) проводить моніторинг роботи інформаційних систем Фонду, у тому числі систем захисту інформації, аналіз електронних журналів роботи (логів, протоколів) з метою виявлення нестандартних ситуацій, збоїв у роботі, спроб несанкціонованого доступу, хакерських атак, інших фактів порушення інформаційної безпеки та вживає відповідних адекватних заходів для запобігання виникненню таких фактів у майбутньому;

7) розробляє та запроваджує разом з департаментом інформаційних технологій політику антивірусного захисту програмного забезпечення, комп'ютерних систем, інформаційних ресурсів, систем обробки і передачі інформації у Фонді;

8) аналізує відповідність стану антивірусного захисту програмного забезпечення, комп'ютерних систем, систем обробки і передачі інформації Фонду політиці антивірусного захисту;

9) узгоджує, контролює та аналізує доступ працівників Фонду до всіх інформаційних ресурсів Фонду: Інтернету, електронної пошти, прикладного, системного та спеціалізованого програмного забезпечення, віддаленого доступу тощо;

10) готує рекомендації (методики) для працівників Фонду стосовно ризиків витоку інформації з обмеженим доступом та шляхів уникнення таких ризиків;

11) планує та організовує роботу із захисту інформації, що є власністю Фонду, інформації з обмеженим доступом, аналізує ефективність роботи щодо забезпечення інформаційної безпеки;

12) розробляє та вдосконалює внутрішні нормативні документи Фонду, що визначають порядок, правила і норми забезпечення інформаційної безпеки Фонду;

13) тестує інформаційні системи Фонду на наявність в них відповідних вразливостей інформаційної безпеки з метою розроблення технологій та/чи рекомендацій щодо їх попередження (мінімізації);

14) здійснює моніторинг та аналіз інформації з питань розробки та випуску технічних засобів захисту інформації нового покоління або їхньої модернізації, обгрунтування пропозицій керівництву Фонду щодо їх закупівлі для потреб Фонду;

15) проводить спеціальні перевірки та інші контрольні заходи відповідно до внутрішніх нормативних документів Фонду, контролює ефективність роботи засобів захисту інформації у Фонді;

16) забезпечує застосування кваліфікованого електронного підпису та використання кваліфікованих електронних довірчих послуг у Фонді, а також банку при здійсненні повноважень під час здійснення ліквідації банку Фондом безпосередньо, шляхом:

ведення актуального цифрового сховища кваліфікованих електронних підписів Фонду;

підготовки для подання кваліфікованому надавачу електронних довірчих послуг інформації, необхідної для отримання кваліфікованих електронних довірчих послуг, пов’язаних з електронним підписом;

надання допомоги працівникам Фонду, яким надано право застосування кваліфікованого електронного підпису (далі – підписувачі), під час генерації їхніх особистих та відкритих ключів;

подання до кваліфікованого надавача електронних довірчих послуг звернень про скасування, блокування посилених сертифікатів відкритих ключів підписувачів;

ведення обліку відкритих ключів підписувачів та носіїв, на яких зберігаються особисті ключі підписувачів;

ведення обліку програмно-апаратних та апаратних носіїв особистих ключів підписувачів;

здійснення зберігання документів та/або їх електронних копій, на підставі яких Фондом та/або підписувачами отримано кваліфіковані електронні довірчі послуги, пов'язані з електронним підписом;

здійснення контролю за використанням підписувачами кваліфікованого електронного підпису та зберіганням ними особистих ключів;

17) обліковує та аналізує результати проведених перевірок, при необхідності письмово інформує за їхніми результатами керівництво Фонду або керівників відповідних структурних підрозділів Фонду;

18) бере участь у проведенні службових перевірок стосовно працівників Фонду з питань порушень у галузі захисту інформації, розробляє пропозиції щодо їх усунення і попередження в майбутньому;

19) організовує та проводить інструктаж і заняття з працівниками Фонду з питань захисту інформації;

20) супроводжує програмний комплекс антивірусного захисту робочих станцій, комплекс забезпечення безпечного підключення до Інтернету, комплекс захисту від вторгнення шкідливих програм та комплекс захисту від витоку даних, програмний комплекс сканер вразливостей;

21) супроводжує програмний комплекс моніторингу інцидентів інформаційної безпеки SIEM (Security Information and Event Management);

22) здіснює моніторинг активності DDoS атак Інтернет-каналів Фонду;

23) при здійсненні повноважень під час здійснення ліквідації банку Фондом безпосередньо вживає заходів щодо унеможливлення неправомірного витоку даних;

24) супроводжує міграцію банківських систем на віртуалізовані ресурси Фонду:

здійснює перевірку та прийом паролів доступу до віртуалізованих банківських систем;

забезпечує керування системою антивірусного захисту віртуалізованих банківських систем;

25) визначає необхідність та здійснює постановку технічних завдань для доопрацювання існуючої функціональності та модернізації вимог інформаційної безпеки щодо інформаційних систем Фонду;

26) здійснює ідентифікацію, оцінку, аналіз ризиків в діяльності Відділу;

27) розробляє методи управління для ідентифікованих Відділом ризиків в порядку визначеному внутрішніми документами Фонду;

28) надає рекомендації щодо визначення ризик-апетиту до інформаційних і технологічних ризиків (в частині інформаційної безпеки) ;

29) проводить аналіз вразливостей, виявлених у ході сканування, на предмет ступеня критичності виявленої вразливості для функціонування інформаційної системи і можливих наслідків при використанні даної вразливості зловмисником;

30) керує системою антивірусного захисту на основі єдиного центру, який забезпечує автоматизований контроль за процесами встановлення, оновлення, конфігурування, пошуку та лікування комп'ютерних вірусів, а також ведення протоколів за фактами вірусних атак та джерел зараження;

31) у сфері захисту об'єктів критичної інфраструктури Фонду:

забезпечує захист об'єктів критичної інфраструктури Фонду в частині створення, налагодження та підтримання функціонування ефективної системи безпеки операційних систем та кібербезпеки;

розробляє, оновлює та забезпечує виконання об'єктових планів заходів кіберзахисту;

проводить навчання та тренінги щодо кібербзахисту об'єктів критичної інфраструктури;

оперативно реагує на протиправні дії, спрямовані на відключення або пошкодження роботи операційних систем;

організовує заходи з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об’єктах критичної інфраструктури Фонду в частині забезпечення безпеки операційних систем та кібербезпеки у взаємодії з іншими суб’єктами національної системи захисту критичної інфраструктури;

забезпечує відновлення функціонування об’єктів критичної інфраструктури Фонду в частині забезпечення безпеки операційних систем та кібербезпеки в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій;

забезпечує негайне інформування уповноваженого органу у сфері захисту критичної інфраструктури України, органів Національної поліції України, Служби безпеки України, інших державних органів про інциденти, пов’язані з порушенням кібербезпеки, а також інформування Служби безпеки України про загрози та ризики актів кібертероризму проти операційних та інших систем об’єктів критичної інфраструктури Фонду, надзвичайних ситуацій або інших небезпечних подій;

забезпечує постійний зв’язок з відповідальними за реагування на протиправні дії та з іншими компетентними організаціями та установами;

забезпечує захист інформації про системи управління, зв’язку та кібербезпеку.

2. Відділ здійснює інші функції, визначені виконавчою дирекцією та директором – розпорядником Фонду.