



Вимоги до захисту інформації при здійсненні переказів грошових коштів

Лектор:
Лимаренко Вячеслав Володимирович
к.т. 066-070-8586

Інформація, що підлягає захисту при здійсненні переказів грошових коштів

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів застосовуються для забезпечення захисту такої інформації (далі – *інформація, що захищається*):

- а) інформації про залишки коштів на банківських рахунках;
- б) інформації про виконані перекази грошових коштів, в тому числі інформації, що міститься в повідомленнях, що стосуються прийому до виконання розпоряджень Учасників, а також в повідомленнях, що стосуються виконання розпоряджень Учасників;
- в) інформації, що міститься в оформлених в рамках застосовуваної форми безготівкових розрахунків розпорядженнях клієнтів Учасників, розпорядженнях Учасників, розпорядженнях платіжного клірингового центру;
- г) інформації про платіжні клірингові позиції;
- д) інформації, необхідної для посвідчення клієнтами права розпорядження грошовими коштами, в тому числі даних власників платіжних карт;
- е) ключової інформації засобів криптографічного захисту інформації, використовуваних при здійсненні переказів грошових коштів;

Інформація, що підлягає захисту при здійсненні переказів грошових коштів

ж) інформації про конфігурацію, яка визначає параметри роботи автоматизованих систем, програмного забезпечення, засобів обчислювальної техніки, телекомунікаційного обладнання, експлуатація яких забезпечується Учасником, Оператором Послуг Платіжної Інфраструктури, банківським платіжним агентом, і використовуються для здійснення переказів грошових коштів, а також інформації про конфігурацію, яка визначає параметри роботи технічних засобів по захисту інформації;

з) інформації обмеженого доступу, в тому числі персональних даних та іншої інформації, що підлягає обов'язковому захисту відповідно до законодавства України, що обробляється при здійсненні переказів грошових коштів.

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів включають в себе:

а) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при призначенні і розподілі функціональних прав і обов'язків осіб, пов'язаних із здійсненням переказів грошових коштів;

б) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації (використання за призначенням, технічного обслуговування і ремонту), модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури;

в) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури, включаючи вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації від несанкціонованого доступу;

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів

г) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації від впливу програмних кодів, що призводять до порушення штатного функціонування засобів обчислювальної техніки;

д) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при використанні інформаційно-телекомунікаційної мережі Інтернет при здійсненні переказів грошових коштів;

е) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при використанні ЗКЗІ;

ж) вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів з використанням взаємопов'язаної сукупності організаційних заходів захисту інформації та технічних засобів захисту інформації, що застосовуються для контролю виконання технології обробки інформації, що захищається при здійсненні переказів грошових коштів;

з) вимоги до організації та функціонування підрозділу, відповідального за організацію і контроль забезпечення захисту інформації;

Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів

- і) вимоги до підвищення обізнаності працівників Учасника, Агента, який є юридичною особою, Оператора Послуг Платіжної Інфраструктури і клієнтів у сфері забезпечення захисту інформації;
- к) вимоги до виявлення інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, і реагування на них;
- л) вимоги до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів;
- м) вимоги до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;
- н) вимоги до доведення Учасником, Оператором Послуг Платіжної Інфраструктури до Оператора інформації про забезпечення в Платіжній Системі захисту інформації при здійсненні переказів грошових коштів;
- о) вимоги до вдосконалення Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури захисту інформації при здійсненні переказів грошових коштів.

Способи виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів

Виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів забезпечується шляхом:

а) вибору організаційних заходів захисту інформації; визначення у внутрішніх документах Учасника, Агента, Оператора, Оператора Послуг Платіжної Інфраструктури порядку застосування організаційних заходів захисту інформації; визначення осіб, відповідальних за застосування організаційних заходів захисту інформації; застосування організаційних заходів захисту; реалізації контролю застосування організаційних заходів захисту інформації; виконання інших необхідних дій, пов'язаних із застосуванням організаційних заходів захисту інформації;

б) вибору технічних засобів захисту інформації; визначення у внутрішніх документах Учасника, Агента, Оператора, Оператора Послуг Платіжної Інфраструктури порядку використання технічних засобів захисту інформації, що включає інформацію про конфігурацію, визначальну параметри роботи технічних засобів захисту інформації; призначення осіб, відповідальних за використання технічних засобів захисту інформації; використання технічних засобів захисту інформації; реалізації контролю за використанням технічних засобів захисту інформації; виконання інших необхідних дій, пов'язаних з використанням технічних засобів захисту інформації.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації. Призначення і розподілі ролей осіб, пов'язаних із здійсненням переказів грошових коштів

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при призначенні і розподілі ролей осіб, пов'язаних із здійсненням переказів грошових коштів, включаються такі вимоги.

а) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують реєстрацію осіб, що володіють правами:

- по здійсненню доступу до інформації, що захищається;
- з управління криптографічними ключами;
- по впливу на об'єкти інформаційної інфраструктури, яке може привести до порушення надання послуг по здійсненню переказів грошових коштів, за винятком банкоматів і платіжних терміналів.

б) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують реєстрацію своїх працівників, що володіють правами щодо формування електронних повідомлень, що містять розпорядження про здійснення переказів грошових коштів.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації. Призначення і розподілі ролей осіб, пов'язаних із здійсненням переказів грошових коштів

в) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують реалізацію заборони виконання однією особою в один момент часу наступних ролей:

- ролей, пов'язаних зі створенням (модернізацією) об'єкта інформаційної інфраструктури та експлуатацією об'єкта інформаційної інфраструктури;
- ролей, пов'язаних з експлуатацією об'єкта інформаційної інфраструктури в частині його використання за призначенням і експлуатацією об'єкта інформаційної інфраструктури в частині його технічного обслуговування і ремонту.

г) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують контроль і реєстрацію дій осіб, яким призначено ролі, визначені в цьому пункті.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації, модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації, модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури, включаються такі вимоги.

- а) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують включення в технічні завдання на створення (модернізацію) об'єктів інформаційної інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів.
- б) Учасник, Агент, який є юридичною особою, Оператор Послуг Платіжної Інфраструктури, участь служби інформаційної безпеки в розробці і узгодженні технічних завдань на створення об'єктів інформаційної інфраструктури.

Учасник, Агент, Оператор Послуг Платіжної Інфраструктури, оператор послуг платіжної інфраструктури забезпечують:

- наявність експлуатаційної документації на використовувані технічні засоби захисту інформації;

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації, модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури

- контроль виконання вимог експлуатаційної документації на використовувані технічні засоби захисту інформації протягом усього терміну їх експлуатації;
 - відновлення функціонування технічних засобів захисту інформації, що використовуються при здійсненні переказів грошових коштів, у випадках збоїв і (або) відмов у їх роботі.
- д) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують реалізацію заборони використання інформації, що захищається на стадії створення об'єктів інформаційної інфраструктури.
- е) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури на стадіях експлуатації та зняття з експлуатації об'єктів інформаційної інфраструктури забезпечують:
- реалізацію заборони несанкціонованого копіювання інформації, що захищається;
 - захист резервних копій інформації, що захищається;

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації на стадіях створення, експлуатації, модернізації, зняття з експлуатації об'єктів інформаційної інфраструктури

- знищення інформації, що захищається в випадках, коли зазначена інформація більше не використовується, за винятком інформації, що захищається, переміщеної в архіви, ведення і збереження яких передбачено законодавчими актами України, нормативними актами НБУ, Правилами та договорами, укладеними Учасником, Агентом, Оператором, Оператором Послуг Платіжної Інфраструктури;
- знищення інформації, що захищається, в тому числі міститься в архівах, способом, що забезпечує неможливість її відновлення.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури, включаються такі вимоги.

а) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують облік об'єктів інформаційної інфраструктури, які використовуються для обробки, зберігання та передачі інформації, що захищається, в тому числі банкоматів і платіжних терміналів.

б) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують застосування некриптографічних засобів захисту інформації від несанкціонованого доступу, в тому числі пройшли в установленому порядку процедуру оцінки відповідності. Допускається застосування некриптографічних засобів захисту інформації від несанкціонованого доступу іноземного виробництва.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури

в) При здійсненні доступу до інформації, що захищається, що знаходиться на об'єктах інформаційної інфраструктури, зазначених вище, Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують:

- виконання процедур ідентифікації, аутентифікації, авторизації своїх працівників під час здійснення доступу до інформації, що захищається;
- ідентифікацію, аутентифікацію, авторизацію учасників платіжної системи при здійсненні переказів грошових коштів;
- визначення порядку використання інформації, необхідної для виконання аутентифікації;
- реєстрацію дій при здійсненні доступу своїх працівників до інформації, що захищається;
- реєстрацію дій, пов'язаних з призначенням та розподілом прав доступу до інформації, що захищається.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури

г) При здійсненні доступу до інформації, що захищається, яка знаходиться на об'єктах інформаційної інфраструктури, зазначених вище, Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують:

- виконання процедур ідентифікації, аутентифікації, авторизації осіб, які здійснюють доступ до програмного забезпечення банкоматів і платіжних терміналів;
- виконання процедур ідентифікації та контроль діяльності осіб, які здійснюють технічне обслуговування банкоматів та платіжних терміналів;
- реєстрацію дій клієнтів, які виконуються з використанням програмного забезпечення, що входить до складу об'єктів інформаційної інфраструктури та використовуваного для здійснення переказів грошових коштів, і автоматизованих систем, що входять до складу об'єктів інформаційної інфраструктури і використовуваних для здійснення переказів грошових коштів, при наявності технічної можливості;

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури

— реєстрацію дій, пов'язаних з призначенням та розподілом прав клієнтів, наданих їм в автоматизованих системах і програмному забезпеченні, при наявності технічної можливості.

д) При здійсненні доступу до інформації, що захищається, яка знаходиться на об'єктах інформаційної інфраструктури, зазначених вище, Учасник забезпечує реєстрацію дій з інформацією про банківські рахунки, включаючи операції відкриття і закриття банківських рахунків.

е) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують:

- реалізацію заборони несанкціонованого розширення прав доступу до інформації, що захищається;
- призначення своїм працівникам мінімально необхідних для виконання їх функціональних обов'язків прав доступу до інформації, що захищається.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури

ж) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури приймають і фіксують у внутрішніх документах рішення про необхідність застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації, призначених для:

- контролю фізичного доступу до об'єктів інформаційної інфраструктури (за винятком банкоматів і платіжних терміналів), збої і відмови в роботі яких призводять до неможливості надання послуг з переказу грошових коштів або до несвоєчасності здійснення переказів грошових коштів, а також доступу до будівлі та приміщення, в яких вони розміщуються;

- запобігання фізичного впливу на засоби обчислювальної техніки, експлуатація яких забезпечуються Учасником, Агентом, Оператором Послуг Платіжної Інфраструктури і які використовуються для здійснення переказів грошових коштів, і телекомунікаційне обладнання, експлуатація якого забезпечується Учасником, Агентом, Оператором Послуг Платіжної Інфраструктури і яке використовується для здійснення переказів грошових коштів, збої і відмови в роботі яких призводять до неможливості надання послуг з переказу грошових коштів або до несвоєчасності здійснення переказів грошових коштів, за винятком банкоматів і платіжних терміналів;

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації при здійсненні доступу до об'єктів інформаційної інфраструктури

- реєстрації доступу до банкоматів, в тому числі з використанням систем відеоспостереження.

з) У разі прийняття Учасником, Агентом, Оператором Послуг Платіжної Інфраструктури рішення про необхідність застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації, зазначених вище, Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують застосування зазначених організаційних заходів захисту інформації та використання технічних засобів захисту інформації, призначених для запобігання несанкціонованому доступу до інформації, що захищається шляхом використання вразливостей програмного забезпечення;

- зниження тяжкості наслідків від впливів на об'єкти інформаційної інфраструктури з метою створення умов для неможливості надання послуг з переказу грошових коштів або несвоєчасність здійснення переказів грошових коштів;

- фільтрацію мережевих пакетів при обміні інформацією між обчислювальними мережами, в яких розташовуються об'єкти інформаційної інфраструктури, і мережею Інтернет.

і) Учасник забезпечує формування для клієнтів рекомендацій щодо захисту інформації від несанкціонованого доступу шляхом використання неправдивих ресурсів мережі Інтернет.

Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ

Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ здійснюється в наступному порядку.

а) Роботи щодо забезпечення захисту інформації за допомогою СКЗІ проводяться відповідно до закону України «Про електронний підпис» (Відомості Верховної Ради України, 2011, №15, ст. 2036; №27, ст. 3880), Положенням про розробку, виробництво, реалізацію та експлуатацію шифрувальних засобів захисту інформації (Положення ПКЗ-2005), затвердженим наказом служби безпеки України та технічною документацією на ЗКЗІ.

б) У випадку якщо Учасник, Агент, Оператор Послуг Платіжної Інфраструктури застосовують ЗКЗІ російського виробника, зазначені ЗКЗІ повинні мати сертифікати уповноваженого державного органу.

Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ

Учасник, Агент, Оператор Послуг Платіжної Інфраструктури застосовують ЗКЗІ, які:

- допускають вбудовування ЗКЗІ в технологічні процеси здійснення переказів грошових коштів, забезпечують взаємодію з прикладним програмним забезпеченням на рівні обробки запитів на криптографічні перетворення і видачі результатів;
- поставляються розробниками з повним комплектом експлуатаційної документації, включаючи опис ключової системи, правила роботи з нею, а також обґрунтування необхідного організаційно-штатної забезпечення;
- підтримують безперервність процесів протоколювання роботи ЗКЗІ і забезпечення цілісності програмного забезпечення для середовища функціонування ЗКЗІ, що представляє собою сукупність технічних і програмних засобів, спільно з якими відбувається штатне функціонування ЗКЗІ і які здатні вплинути на виконання пропонованих до ЗКЗІ вимог.

в) У разі застосування ЗКЗІ Учасник, Агент, Оператор Послуг Платіжної Інфраструктури визначають у внутрішніх документах і виконують порядок застосування ЗКЗІ, що включає:

- порядок введення в дію, включаючи процедури вбудовування ЗКЗІ в автоматизовані системи, які використовуються для здійснення переказів грошових коштів;

Захист інформації при здійсненні переказів грошових коштів з використанням ЗКЗІ

- порядок експлуатації ЗКЗІ;
- порядок відновлення працездатності ЗКЗІ у випадках збоїв і (або) відмов у їх роботі;
- порядок внесення змін до програмного забезпечення ЗКЗІ і технічну документацію на ЗКЗІ;
- порядок зняття з експлуатації ЗКЗІ;
- порядок управління ключовою системою;
- порядок поводження з носіями криптографічних ключів, включаючи порядок застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації, призначених для запобігання несанкціонованого використання криптографічних ключів, і порядок дій при зміні і компрометації ключів.

г) Криптографічні ключі виготовляються клієнтом, Оператором Послуг Платіжної Інфраструктури і Учасником.

д) Безпека процесів виготовлення криптографічних ключів ЗКЗІ забезпечується комплексом технологічних заходів захисту інформації, організаційних заходів захисту інформації та технічних засобів захисту інформації відповідно до технічної документації на ЗКЗІ.

е) Оператор визначає необхідність використання СКЗІ, якщо інше не передбачено законами та іншими нормативними правовими актами України.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації з використанням технологічних заходів захисту інформації

До складу вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації з використанням технологічних заходів захисту інформації, включаються такі вимоги.

а) Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують облік і контроль Оператор визначає порядок застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації, що використовуються при проведенні операцій обміну електронними повідомленнями та іншою інформацією при здійсненні переказів грошових коштів. Учасник і Оператор Послуг Платіжної Інфраструктури забезпечують виконання зазначеного порядку.

в) Розпорядження клієнта, розпорядження Учасника та розпорядження ЦПКК в електронному вигляді може бути посвідчений електронним підписом, а також відповідно до пункту 3 статті 847 Цивільного кодексу України (Відомості Верховної Ради України, 1996, №5, ст. 410) аналогами власноручного підпису, кодами, паролями та іншими засобами, що дозволяють підтвердити складання розпорядження уповноваженою на це особою.

Склад вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються для захисту інформації з використанням технологічних заходів захисту інформації

г) При експлуатації об'єктів інформаційної інфраструктури Учасник, Агент, Оператор Послуг Платіжної Інфраструктури забезпечують:

- ✓ захист електронних повідомлень від спотворення, фальсифікації, переадресації, несанкціонованого ознайомлення та знищення, помилкової авторизації;
- ✓ контроль дотримання встановленої технології підготовки, обробки, передачі та зберігання електронних повідомлень і інформації, що захищається на об'єктах інформаційної інфраструктури;
- ✓ аутентифікацію вхідних електронних повідомлень;
- ✓ взаємну аутентифікацію учасників обміну електронними повідомленнями;
- ✓ відновлення інформації про залишки коштів на банківських рахунках і даних власників платіжних карт в разі умисного руйнування або спотворення або виходу з ладу засобів обчислювальної техніки;
- ✓ звірку вихідних електронних повідомлень з відповідними вхідними і обробленими електронними повідомленнями при здійсненні розрахунків в платіжній системі;
- ✓ виявлення фальсифікованих електронних повідомлень, в тому числі здійснення операцій, пов'язаних із здійсненням переказів грошових коштів, зловмисником від імені авторизованого клієнта (підміна авторизованого клієнта) після виконання процедури авторизації.

Склад вимог до організації та функціонування служби інформаційної безпеки

До складу вимог до організації та функціонування служби інформаційної безпеки включаються такі вимоги.

- а) Учасник, Агент, який є юридичною особою, Оператор Послуг Платіжної Інфраструктури:
- забезпечують формування служби інформаційної безпеки, а також визначають у внутрішніх документах цілі і завдання діяльності цієї служби;
 - надають повноваження і виділяють ресурси, необхідні для виконання службою інформаційної безпеки встановлених цілей і завдань.

б) Учасник, Оператор Послуг Платіжної Інфраструктури призначають куратора служби інформаційної безпеки зі складу свого органу управління і визначають його повноваження. При цьому служба інформаційної безпеки і служба інформатизації не повинні мати загального куратора.

- в) Учасник, який має філії:
- забезпечує формування служб інформаційної безпеки в зазначених філіях, визначає для них необхідні повноваження і виділяє необхідні ресурси;
 - забезпечує взаємодію та координацію робіт служб інформаційної безпеки.

Склад вимог до організації та функціонування служби інформаційної безпеки

г) Служба інформаційної безпеки здійснює планування і контроль забезпечення захисту інформації при здійсненні переказів грошових коштів, для чого наділяється такими повноваженнями:

- здійснювати контроль виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;
- визначати вимоги до технічних засобів захисту інформації та організаційним заходам захисту інформації;
- контролювати виконання працівниками вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;
- брати участь в розглядах інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, і пропонувати застосування дисциплінарних стягнень, а також надсилати пропозиції щодо вдосконалення захисту інформації;
- брати участь в діях, пов'язаних з виконанням вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, що застосовуються при відновленні надання послуг платіжної системи після збоїв і відмов в роботі об'єктів інформаційної інфраструктури.

Склад вимог до підвищення обізнаності в галузі забезпечення захисту інформації

До складу вимог до підвищення обізнаності в галузі забезпечення захисту інформації включаються такі вимоги:

а) Учасник, Агент, який є юридичною особою, Оператор Послуг Платіжної Інфраструктури забезпечують підвищення обізнаності працівників в сфері забезпечення захисту інформації:

- по порядку застосування організаційних заходів захисту інформації;
- по порядку використання технічних засобів захисту до забезпечення захисту інформації при здійсненні переказів грошових коштів.

б) Учасник і Оператор Послуг Платіжної Інфраструктури забезпечують виконання зазначених у цьому підпункті вимог.

- в) Учасник, Агент (Субагент), Оператор Послуг Платіжної Інфраструктури забезпечують:
- застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації, призначених для виявлення інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;

Склад вимог до підвищення обізнаності в галузі забезпечення захисту інформації

- інформування служби інформаційної безпеки, в разі її наявності, про виявлення інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;
- реагування на виявлені інциденти, пов'язані з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;
- аналіз причин виявлених інцидентів, пов'язаних з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів, проведення оцінки результатів реагування на такі інциденти.

г) Оператор забезпечує облік і доступність для Учасників і Операторів Послуг Платіжної Інфраструктури, що залучаються для надання Послуг Платіжної Інфраструктури в Платіжній Системі, інформації:

д) про виявлені в Платіжній Системі інциденти, пов'язані з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів;

е) про методики аналізу і реагування на інциденти, пов'язані з порушеннями вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів.

Склад вимог до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів грошових коштів

До складу вимог до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів грошових коштів включаються такі вимоги:

а) Документи, що становлять порядок забезпечення захисту інформації при здійсненні переказів грошових коштів, визначають:

- склад і порядок застосування організаційних заходів захисту інформації;
- склад і порядок використання технічних засобів захисту інформації, включаючи інформацію про конфігурацію технічних засобів захисту інформації, що визначає параметри їх роботи;
- порядок реєстрації та зберігання інформації на паперових носіях і в електронному вигляді, що містить підтвердження виконання порядку застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації.

б) Оператор встановлює розподіл обов'язків щодо визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів шляхом:

- самостійного визначення Оператором порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;

Склад вимог до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів грошових коштів

— розподілу обов'язків щодо визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів між Оператором, Операторами Послуг Платіжної Інфраструктури і Учасниками;

в) Оператор, Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів в рамках розподілу обов'язків, встановлених оператором платіжної системи.

г) Для визначення порядку забезпечення захисту інформації при здійсненні переказів грошових коштів Оператор, Учасник, Оператор Послуг Платіжної Інфраструктури в рамках обов'язків, встановлених Оператором, можуть використовувати:

- положення національних стандартів щодо захисту інформації, стандартів організацій, в тому числі стандартів НБУ, рекомендацій в галузі стандартизації, в тому числі рекомендацій НБУ, прийнятих відповідно до законодавства України про технічне регулювання;
- положення документів, визначених міжнародними платіжними системами;

Склад вимог до визначення і реалізації порядку забезпечення захисту інформації при здійсненні переказів грошових коштів

– результати аналізу ризиків при забезпеченні захисту інформації при здійсненні переказів грошових коштів на основі моделей загроз і порушників безпеки інформації, визначених у національних стандартах щодо захисту інформації, стандартах організацій, в тому числі стандартах НБУ, прийнятих відповідно до законодавства України про технічне регулювання, або на основі моделей загроз і порушників безпеки інформації, визначених Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури.

д) Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів.

е) Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують призначення осіб, відповідальних за виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів.

ж) Служба інформаційної безпеки Учасника, Оператора Послуг Платіжної Інфраструктури здійснює контроль виконання порядку забезпечення захисту інформації.

Склад вимог до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів

До складу вимог до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів включаються такі вимоги:

а) Учасник, Оператор, Оператор Послуг Платіжної Інфраструктури забезпечують проведення оцінки виконання вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів.

б) Оцінка відповідності здійснюється на основі:

- інформації на паперовому носії та в електронному вигляді, що містить підтвердження виконання порядку застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації;
- аналізу відповідності порядку застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації вимогам законодавства України;
- результатів контролю виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів.

Склад вимог до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів

в) Оцінка відповідності здійснюється Учасником, Оператором, Оператором Послуг Платіжної Інфраструктури самостійно або із залученням сторонніх організацій.

г) Оператор, Учасник, Оператор Послуг Платіжної Інфраструктури забезпечують проведення оцінки відповідності не рідше одного разу на два роки, а також на вимогу НБУ зі змінами, внесеними до законодавчих актів, нормативні акти Банку України, що регулюють відносини в національній платіжній системі.

б) Учасник, Оператор Послуг Платіжної Інфраструктури регламентують порядок вжиття заходів, спрямованих на вдосконалення захисту інформації при здійсненні переказів грошових коштів, у випадках:

- зміни вимог до захисту інформації, визначених Правилами;
- змін, внесених до законодавчих актів України, нормативні акти НБУ, що регулюють відносини в національну платіжну систему;
- зміни порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;

Склад вимог до оцінки виконання Оператором, Учасником, Оператором Послуг Платіжної Інфраструктури вимог до забезпечення захисту інформації при здійсненні переказів грошових коштів

- виявлення загроз, ризиків і вразливостей в забезпеченні захисту інформації при здійсненні переказів грошових коштів;
- виявлення недоліків при здійсненні контролю виконання порядку забезпечення захисту інформації при здійсненні переказів грошових коштів;
- виявлення недоліків при проведенні оцінки відповідності.

в) Прийняття рішень Учасник, Оператора Послуг Платіжної Інфраструктури щодо вдосконалення захисту інформації при здійсненні переказів грошових коштів узгоджується зі службою інформаційної безпеки.

A blue key is positioned diagonally across the frame. The background is a light blue gradient with a pattern of binary code (0s and 1s) in a darker blue, creating a digital or technological theme. The key has a standard notched profile and a simple loop handle.

Дякую за увагу
Лекцію закінчено