

МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАХИСТУ ТА БЕЗПЕКИ ІНФОРМАЦІЇ ПРИ ЗАСТОСУВАННІ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Розвиток сучасних інформаційних технологій, загальна автоматизація та комп'ютеризація, різке збільшення кількості інформаційно-комунікаційних систем і мереж призвели до того, що інформаційна безпека не тільки стає обов'язковою, вона ще й одна з характеристик інформаційних систем.

Безпека інформації (при застосуванні інформаційних технологій) (англ. ITsecurity) - стан захищеності інформації (даних), що забезпечує безпеку інформації, для обробки якої вона застосовується, і інформаційну безпеку автоматизованої інформаційної системи, в якій вона реалізована [1].

При організації ефективного та надійного захисту при застосуванні сучасних інформаційних технологій потрібно керуватися системою принципів. Під принципами захисту інформації розуміються основні ідеї і найважливіші рекомендації з питань організації та здійснення робіт для ефективного захисту інформаційних ресурсів інформаційно – комунікаційних систем і мереж. Використання даних принципів дозволяє ефективно організувати роботу з захисту інформації (табл.1) [2].

Таблиця 1

Система принципів організації захисту інформації при застосуванні інформаційних систем

Принципи	Характеристика
<p style="text-align: center;"><u>Правові:</u></p> <ul style="list-style-type: none"> - легітимність (законність); - пріоритет міжнародного права над внутрішньодержавним; - економічна доцільність. 	<p>Базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а також гарантують їх здійснення. Ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкту правовідносин.</p>
<p style="text-align: center;"><u>Організаційні:</u></p> <ul style="list-style-type: none"> - науковий підхід до організації захисту інформації; - планування захисту ; - керування системою захисту; - безперервність процесу захисту інформації; - мінімальна достатність організації захисту; - комплексний підхід до організації захисту інформації; - відповідність рівня захисту цінності інформації; - гнучкість захисту; - багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; - багаторубіжність захисту інформації; - обмеження числа осіб, які допускаються захищеної інформації; - особиста відповідальність персоналу за збереження довіреної інформації 	<p>Роль організаційного захисту інформації в системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.</p>

Безпека автоматизованої інформаційної системи (АІС) - стан захищеності автоматизованої системи, при якому забезпечуються конфіденційність, доступність, цілісність, підзвітність і справжність її ресурсів (табл.2).

Таблиця 2

Принципи безпеки автоматизованої інформаційної системи

Принцип	Ознака загрози
конфіденційність	стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на неї право
доступність	уникнення тимчасового або постійного приховування інформації від користувачів, які отримали права доступу
цілісність	уникнення несанкціонованої модифікації інформації
підзвітність	забезпечення ідентифікації суб'єкта доступу та реєстрації його дій
справжність ресурсів АІС	властивість, що гарантує, що суб'єкт або ресурс ідентичні заявленим

Отже, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. Безпеку інформаційних систем можна охарактеризувати як стан забезпеченості необхідних умов і параметрів інформаційних процесів, що реалізуються за їх допомогою, від негативного впливу ззовні. Сутність викладеного дає підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

Список використаних джерел:

1. Системи забезпечення інформаційної безпеки [Електронний ресурс]: Режим доступу: <https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review>
2. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП ІНТЕРСЕРВІС», 2009. – 716 с
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] : Режим доступу : <http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>

Гриневич М.А., студентка гр.ФК-21

Научный руководитель – Башлакова О.С., к.э.н., доцент

Гомельский Государственный университет имени Франциска Скорины (г.Гомель, Беларусь)

**ПЕРСПЕКТИВЫ РАЗВИТИЯ И ИСПОЛЬЗОВАНИЯ
ТЕХНОЛОГИИ БЛОКЧЕЙН И КРИПТОВАЛЮТ В БАНКОВСКОМ СЕКТОРЕ**

Блокчейн является сегодня практически самой прогрессивной и стремительно развивающейся технологией, представляющей собой базу данных, в которой хранится информация о каждой экономической транзакции, произведенной в этой системе. Безопасно храниться может не только информация, но и почти все виды финансовых активов. Информацию базы данных невозможно подделать, так как ее копии одновременно хранятся на всех компьютерах системы, и каждый ее участник имеет к ней доступ.

Традиционно как наиболее развитый финансовый институт банковский сектор стремится использовать различные инновационные технологии для привлечения клиентов, которые желают иметь быстрый и максимально легкий доступ к услугам и транзакциям. Однако для дальнейшего сохранения своей конкурентоспособности на рынке банкам следует эффективно использовать платформу блокчейн, на основе функционирования которой они смогут сохранить конкурентоспособность на финансовом рынке, рыночную позицию при наметившейся тенденции увеличения финансовых операций так называемых «неискушенных инвесторов», повысить эффективность своей деятельности, оптимизировать функции бэк-офиса, а также снизить риски. При этом наиболее безопасным вариантом развития данной технологии является использование смарт-контрактов, которые представляют собой компьютерный алгоритм, усиливающий безопасность сделок в блокчейне.

Компания Accenture недавно опубликовала отчет, в котором утверждается, что технология блокчейн может снизить затраты на инфраструктуру для восьми из 10 крупнейших инвестиционных банков в мире в среднем на 30 процентов. Девять из 10 банковских специалистов из опрошенных крупных американских, европейских и канадских коммерческих банков заявили, что они в настоящее время изучают использование технологии блокчейн для платежей [1]. Национальный банк Республики Беларусь также в тестовом режиме запустил использование данной технологии.

Блокчейн является платформой функционирования цифровой денежной единицы – криптовалюты. Initial coin offering (ICO) – форма предложения криптовалют. Кроме того, на данный момент ICO можно рассматривать как альтернативу венчурному финансированию. Токены могут представлять собой варианты контрактов и договоров, купоны на продукцию, новые виды денег. Чаще всего они бывают аналогом ценных бумаг (в большинстве случаев – разновидностью акций, которые могут давать владельцу на привилегии в использовании сервиса и технологии). Токенизация акций позволяет сделать их более ликвидными, гибкими и прозрачными, чем обычные ценные бумаги. Работа с токенами, как и с криптовалютами, проходит без посредников, что увеличивает скорость и безопасность операции, уменьшает издержки. Также токенизация ценных бумаг приведет к увеличению объема вложений, оптимизирует эффективность управления, ликвидность активов в процессе их хранения или передачи. Токенизация – это переход к цифровой экономике, к прозрачной и безопасной работе с активами в режиме реального времени.

Банк может фиксировать, например, все ипотечные кредиты, проходящие через систему блокчейн, разбивая денежный поток на смарт-контракты, проверяемые в режиме реального времени. В этом случае аудиторы смогут увидеть внесение первых платежей и уплату остальных взносов, в результате чего сократится время на оценку кредитных рисков. Здесь блокчейн будет являться платформой взаимодействия всех агентов, а также будет фиксировать данную электронную сделку. Банк может осуществить кредитование быстро и уменьшить издержки по переводу денежных средств.

На пространстве блокчейн банковские кредитно-финансовые организации могут размещать свои бонусные программы для всех участников. Для банков особенностью будет выступать то, что ведение этих программ осуществляется без централизованной инфраструктуры, а также возможности доступа к бонусным программам других банков. Тогда клиент банка, который получил бонусы за совершение определенной операции, сможет продать или обменять их на бонусы другой компании. При этом банки или компании смогут принимать бонусы без заключения договоров.

Оформление и осуществление платежей в финансовой сфере, в том числе и на фондовых рынках, чаще всего является затратоёмкой операцией, так как каждая организация в процессе транзакции должна вести учет