Таблица 2

**Варианты учёта криптовалют у субъекта хозяйствования в мировой практике**

| Варианты использования | Ценная бумага | Товароматериальная ценность (актив организации) | Локальная валюта (например, в Германии) |
|---|---|---|---|
| 1.Изменение курса криптовалюты при операциях их купли-продажи | а) не подлежит переоценке (поэтому до продажи не является объектом налогообложения);<br>б) при продаже определяется прибыль от операций с ценными бумагами, из которой уплачивается налог на прибыль | а) не подлежит переоценке (поэтому до продажи не является объектом налогообложения);<br>б) при продаже уплачивается НДС по установленной ставке, определяется прибыль от операций от продажи ТМЦ, из которой уплачивается налог на прибыль | а) подлежит переоценке (поэтому возникают курсовые разницы, облагаемые налогом на прибыль – при положительной величине);<br>б) при продаже автоматически рассчитывается курсовая разница, с которой уплачивается налог на прибыль. Поскольку отсутствует официальный курс, установленный центральным банком (как по иным иностранным валютам), налог на прибыль будет уплачиваться с разницы курсов между датами приобретения и продажи |
| 2. Использование криптовалюты в качестве средства платежа за реализуемые товары (работы, услуги) | уплачивается НДС и налог на прибыль | уплачивается НДС и налог на прибыль (по аналогии с бартером) | уплачивается НДС и налог на прибыль, возникают курсовые разницы |
| | В связи с существующей неопределенностью правового статуса криптовалют в некоторых странах в настоящее время при реализации товаров (работ, услуг) за криптовалюты клиенту может быть сделана 99-процентная скидка от стоимости товара (работы, услуги), при этом продавец уплачивает добровольно налоги от всей суммы без учета скидки, а покупатель 1 % стоимости оплачивает в национальной валюте, а 99% - криптовалютой. Это позволяет избежать необходимости уплаты подоходного налога от подарка покупателем (если криптовалюты не являются законным средством платежа, есть риск, что контролирующие органы воспримут такую сделку как дарение, что вызовет необходимость уплаты подоходного налога для физлиц). А при такой схеме дарения нет, а продавец уплачивает НДС и налог на прибыль от всей суммы сделки, получив при этом криптовалюту. А поскольку криптовалюта не является законным средством платежа и узаконенной ценностью, то для продавца это не рассматривается как дарение | | |

Можно сделать вывод о том, что на сегодняшний день технология блокчейн стремительно развивается. Данная технология только начинает использоваться в банковской системе, ее области применения многогранны и постоянно увеличиваются, что позволяет кредитным организациям улучшить процесс совершения операций. Блокчейн гарантирует законность проведенных транзакций через запись их в распределенной системе реестров, которые связаны между собой защищенным механизмом проверки. Криптовалюты пока развиваются по принципу ограниченных природных ресурсов (например, золота), их дальнейшее развитие сегодня становится просто неизбежным при решении проблем с медленной скоростью транзакций, ограничения легализации незаконно полученных доходов, легализации деятельности криптоплатформ и криптобирж.

**Список использованных источников**

1. Данные компании Accenture «Join the blockchain party. How banks are building a real-time global payment network». – [Электронный ресурс]. – Режим доступа: https://www.accenture.com/us-en/insight-blockchain-technology-how-banks-building-real-time.

2. Декрет №8 Президента Республики Беларусь от 21.12.2017 «О развитии цифровой экономики». – [Электронный ресурс]. – Режим доступа: http://president.gov.by/ru/official_documents_ru/view/dekret-8-ot-21-dekabrja-2017-g-17716/.

3. Постановление Правления Национального банка Республики Беларусь от 15.02.2018 № 62. – [Электронный ресурс]. – Режим доступа: https://normativka.by/news/show/30657/.

**Домашенко С.В.,** 1 курс магістратури МЕКп-171,
**Акименко А.М.,** к.ф.-м.н., професор
*Чернігівський національний технологічний університет (м. Чернігів, Україна)*

## ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КІБЕРЗАГРОЗ

Сучасний розвиток технологій супроводжується збільшенням кількості кібератак, злочинів у мережі Інтернет, порушення роботи державних та приватних установ. Зважаючи на це організації практично у всіх сферах діяльності повинні оперативно реагувати на кіберзагрози та належним чином протидіяти кібератакам.

Згідно Закону України «Про основні засади забезпечення кібербезпеки України» кібератака це – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та

технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [1].

За даними які опубліковані у звіті з інформаційної безпеки за 2017 рів від компанії Cisco, приблизно в кожному четвертому випадку організація, що піддалася атаці, втрачає бізнес-можливості. Четверо з десяти опитаних повідомляло, що подібні втрати мали велике значення. Кожна п'ята організація втратила замовників внаслідок кібератак [2]. Україну кіберзлочинність не оминула, за 2016 рік було здійснено 247 кібератаки на системи органів державної влади [3]. Згідно даних компанії Trend Micro Incorporated за першу половину 2017 року було зафіксовано більше 82 млн. атак з використання програм-вимагачів, а також 3 тис. спроби здійснення шахрайства з використанням корпоративної пошти (BEC).

В наші дні є три основні типи кібератак, а саме атаки на конфіденційність в мережі, її цілісність та її доступність.

Автори атак, націлені на порушення конфіденційності, хочуть викрасти або виставити у відкритий доступ інформацію, таку як: номера кредитних карток або соціального страхування, отриманих незаконним способом.

Другий тип атак пов’язаний з доступністю мережі – ці атаки біль відомі під назвою «відмова в обслуговувані» (denial-of-service, DoS) або «розподіленої відмови в обслуговувані» (distributed-denial-of-service, DDoS). Атаки данного типу зазвичай направлені на блокування роботи мережі шляхом надісланню їй великої кількості запитів, що приводять до її обвалу. На сьогодні відомі такі DDos атаки як: DDos атаки з використанням ботнетів, DDos атаки з використанням SSL з’єднаня.

Також кібератаки можуть впливати на цілісність мережі. Можна сказати, що такий тип атак частково є «фізичним». Вони націлені на зміну чи знищення комп'ютерних програм, а також на пошкодження устаткування, інфраструктури або інших систем в реальному світі. Після того як комп'ютер або інший пристрій піддається подібній атаці, такий пристрій стає повністю непотрібним.

Дослідники з французького інституту INRIA розробили новий метод атак на системи шифрування, які застосовують 64-бітові блокові шифри 3DES та Blowfish. Цей метод отримав кодове ім’я Sweet32. З його допомогою можна отримати cookie, використовуються для аутентифікації з зашифрованого 3DES HTTPS-трафіку, а також відновлювати імена користувачів і паролі з зашифрованого за допомогою Blowfish трафіку, що передається через VPN [4].

Отже, кібератаки несуть в собі величезну небезпеку не тільки для компаній, а й для держав. Тому держава повинна сприяти приєднанню наукових та навчальних установ, організацій, громадських об’єднань для впровадження певних заходів для усунення кіберзагроз та кібератак.

**Список використаних джерел**

1. Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VII [Електро- нний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2163-19.

2. Cisco. Річний звіт з інформаційної безпеки, 2017. [Електронний ресурс]. – Режим доступу: http://www.cisco.com/c/dam/m/digital/elqcmcglobal/with/1301152/ReportUKR.pdf.

3. Служба безпеки України [Еклетронний ресурс]. – Режим доступу: https://ssu.gov.ua/ua/news/1/category/2/view/2474#sthash.4E1VYLlG.dN4fEV OL.dpbs.

4. Sweet32: Birthday attacks on 64-bit block ciphers in TLS and open VPN [Електронний ресурс]. – Режим доступу: https://sweet32.info.

5. Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей II Міжнародної науково-практичної конференції, 20-22 квітня 2017 року, м. Кропивницький: ЦНТУ, 2017. – 211 с.

6. Индустрии будущего / Алек Росс ; [пер. с англ. П. Мироно-ва]. – Москва : Издательство АСТ, 2017. – 287с.

**Ігнатенко О.П.,** студент 1 курсу, група МЕКп-171
Науковий керівник - Акименко А.М., к.ф.-м.н., професор
*Чернігівський національний технологічний університет*

## РОЗПІЗНАВАННЯ ТЕКСТУ ТА ЙОГО МЕТОДИ

Тема розпізнавання тексту потрапляє під розділ розпізнавання образів. І для початку коротко про саме розпізнаванні образів.

Розпізнавання тексту або теорія розпізнавання образів це розділ інформатики та суміжних дисциплін, що розвиває основи і методи класифікації та ідентифікації предметів, явищ, процесів, сигналів, ситуацій тощо об'єктів, які характеризуються кінцевим набором деяких властивостей і ознак.

Також вона стверджує, що можна виділити два основних напрямки:

- Вивчення здібностей до розпізнавання, якими володіють живі істоти, пояснення та моделювання їх;
- Розвиток теорії та методів побудови пристроїв, призначених для вирішення окремих завдань в прикладних цілях.