Ключові слова: кіберзлочинність, міжнародний стандарт, криміналізація, спосіб вчинення кіберзлочинів, політика кібербезпеки.
Ключевые слова: киберпреступность, международный стандарт, криминализация, способ совершения киберпреступлений, политика кибербезопастности.
Keywords: cybercrime, international standard, criminalization, method of committing cybercrimes, cybersecurity policy.

***Науковий керівник**: к.ю.н., доцент Дикий О. В.*

Керусов Максим Вікторович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ ПРОВАЙДЕРІВ

Термін інформаційна безпека в сучасному світі надзвичайно широкий. Вон включає в себе як контроль за непоширенням інформації, яка вважається секретною, так і облік своєчасного, повного і якісного інформування громадян про події в країні і світі, вільний доступ до різних джерел інформації – і в той же час просування цілісності суспільства, підтримання його морального благополуччя, захист від різноманітних несприятливих інформаційних впливів.

Актуальність порушення проблеми захисту інформаційної безпеки обумовлюється зростанням доступу до мереж загального користування окремих категорій негативно настроєних осіб, певною уразливістю окремих мереж, збільшенням спроб злочинних елементів на здобування або руйнування інформації, а також збільшення кількості шахраїв які намагаються вкрасти персональні данні.

Політика інформаційної безпеки являє собою набір обмежень, вимог, рекомендацій, правил, які регламентують порядок інформаційної діяльності в організації і направлені на досягнення і підтримку стану інформаційної безпеки в організації.

Також можна сказати що під політикою інформаційної безпеки розуміється набір законів, обмежень, правил і рекомендацій, які регламентують порядок опрацювання інформації і направлені на захист інформації від певних загроз

Причиною появи політики інформаційної безпеки є вимога до такого документа від регулятора – організації, яка визначає правила функціонування підприємств цієї галузі. У цьому випадку відсутність політики інформаційної безпеки може призвести до репресивних дій проти підприємства або навіть до повного припинення його діяльності. Крім того, галузеві або загальні, місцеві чи міжнародні стандарти мають конкретні вимоги або керівні принципи.

Відсутність політики інформаційної безпеки викликає негативну оцінку, що в свою чергу впливає на публічні показники підприємства – позицію в рейтингу, рівень надійності тощо.

На мою думку політику інформаційної безпеки умовно можна розділити на 2 напрямки:

– Законодавче закріплені акти які мають бути застосовані усіма провайдерами. До них можна віднести: указ президента України № 47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Рішення НКРЗІ № 22 від 15.01.2019 Про надання операторам, провайдерам телекомунікацій рекомендації щодо поширення серед користувачів правил безпеки в кіберпросторі, Закон, ВР України, від 18.11.2003, № 1280-IV «Про телекомунікації»

– Розробка провайдером власної політики інформаційної безпеки.

У деяких користувачів може виникнути питання: що може розробляти провайдер якщо основні положення заложенні законодавчими актами (закон про телекомунікації глави VI споживачі телекомунікаційних послуг і VII оператори, провайдери телекомунікацій (саме в них вказані права і обов'язки споживачів і операторів)).

На свій розгляд інтернет провайдери залишають:

– постачання додаткових послуг та їх оплату;

– з метою захисту інтересів абонентів і мережі оператори міжміського (міжнародного) телефонної мережі можуть здійснювати, при наявності необхідного програмного забезпечення і технічних засобів, оперативний контроль використання послуг з кожного телефону (моніторинг);

– в разі різких відхилень (обсяги, види послуг і т.д.) Оператор може вжити заходів для виявлення їх причин (можливе стороннє підключення, неузгоджене використання телефону і т.д.)

У наш час інформаційні технології постійно розвиваються, що призводить до появи нових ризиків та загроз. Однак основними проблемами, що виникають сьогодні в процесі захисту порушених прав, є складність встановлення порушника, складність реалізації заходів реагування, враховуючи екстериторіальний характер Інтернету, а також підтримка балансу між реакціями на порушення та збереження свободи в інформаційному просторі.

Складнощі з встановленням особи злочинця пов'язані з особливостями Інтернету, в якому від більшості користувачів не потрібно повідомляти особисті дані. Регулярно з'являються ініціативи щодо впровадження більш повної ідентифікації, в тому числі у вигляді змін у законодавстві. До них відносяться неодноразові пропозиції зареєструвати веб-сайти, аналогічні традиційним ЗМІ. Однак в більшості випадків такі ініціативи відкидаються через значне громадського спротиву. Їх введення загрожує перетворенням в механізм цензури.

Однак в деяких випадках держава залишає за собою вирішальний голос стосовно користування веб ресурсами як приклад можна навести Указом Президента України від 15,05,2017 року Ш 133/2017 введено у дію рішення РНБО щодо обмеження діяльності в Україні російських соціальних мереж та сервісів. У даному переліку 52 російських сайти, щодо яких вжито санкційні заходи.

Отже можна зробити висновок що хоча політика інформаційної безпеки у інтернет провайдерів може відрізнятися

проте основні пункти в них будуть однакові – ті що вказані в закріплених законодавчих актах.

Список використаних джерел:

1. закон України Про телекомунікації: офіц. веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/1280–15#Text
2. Укртелеком офіц. веб-сайт. URL: https://ukrtelecom.ua/reference/zakhist-personalnikh-danikh/

Ключові слова: політика інформаційної безпеки, інформаційна безпека, інформаційна безпека в інтернеті.

Ключевые слова: политика информационной безопасности, информационная безопасность, информационная безопасность в интернете.

Keywords: information security policy, information security, information security on the Internet.

***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*

Малюта Владислав Васильович
Національний університет «Одеська юридична академія»,
студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

СМАРТ-КОНТРАКТ ЯК ГАРАНТІЯ БЕЗПЕКИ ДОГОВІРНИХ ПРАВОВІДНОСИН

Актуальність обраної теми дослідження слід розглядати в нерозривній сукупності ознак, що дозволяють визначити тему як актуальну. Такими ознаками є: відповідність сучасному стану наукового дослідження, відповідність тенденціям розвитку наукової думки, практична обґрунтованість теми.

Дану тему прямо або опосередковано розглядали в своїх роботах такі науковці як Савельєв А. І., Баранов О. А., Лещенко Д., Коваленко С. та інші. На даний момент реалізація технології смарт-контрактів є можливою як технічно, так і юридично, проте безпосереднього правового оформлення смарт-контракти ще не отримали, що дає можливість ствер-