$$A = m\sqrt{2gRV_0}$$

Отримана формула для роботи А рухливої ваги дозволяє отримати закон зміни механічної енергії автомобільного колеса:

$$mgR + \frac{mv^2}{2} - \frac{mv_0^2}{2} = m\sqrt{2gRV_0}$$

Тоді шляхом рішення наведеного рівняння, відносно швидкості рухливої ваги в зоні плями контакту автомобільного колеса з опорною поверхнею, отримуємо формулу швидкості для автомобільного колеса:

$$v = V_0 + \sqrt{2gR}$$

Література:

1. Петров Л. «Спосіб переміщення мобільного енергетичного засобу». 2015. Бюл. № 1.

2. Петров Л. «Спосіб переміщення мобільного засобу» 2014. Бюл. № 1.

3. Лобас Л. Лобас Л. Теоретична механіка: Підручник для студентів вищих технічних навчальних закладів. К.: ДЕТУТ. 2008. С. 331-335.

DOI https://doi.org/10.30525/978-9934-26-266-1-46

ДЕЯКІ ОСОБЛИВОСТІ ЮРИДИЧНИХ КРИТЕРІЇВ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кобко Євген Васильович

кандидат юридичних наук, доцент,
професор кафедри публічного управління та адміністрування
Національна академія внутрішніх справ
м. Київ, Україна

Ніцевич Олеся Володимирівна

аспірант
Науково-дослідний інститут публічного права
м. Київ, Україна

Сьогодні розвиток суспільства супроводжується економічною глобалізацією, урбанізацією та широким застосуванням інформаційних

технологій. А особливо в останні місяці повномасштабного вторгнення росії питання критичної інфраструктури постає особливої уваги.

Тільки ті країни, які мають розвинену інфраструктуру, здатні стати сучасними економічними центрами, розвивати та зосереджувати на своїй території фінансові, промислові та інтелектуальні потужності. У той же час помітною є тенденція до посилення негативних процесів природного, техногенного та соціально-політичного характеру (в світі збільшується кількість та масштаб наслідків природних катастроф, тліють та розгораються нові військові конфлікти, постійно здійснюються терористичні акти, надшвидкими темпами зростає кількість кібер-атак), що зумовлюють прямі та каскадні загрози для стабільного функціонування згаданих інфраструктур, а отже забезпечення їх «абсолютного захисту» стає непосильним завданням навіть для економічно розвинутих держав.

Саме необхідність зосередження ресурсів на захисті найбільш життєво важливих інфраструктурних об'єктів обумовила розвиток та впровадження концепції критичної інфраструктури (КІ) як складової систем забезпечення національної безпеки низки провідних країн світу. В США до КІ відносять системи, мережі та окремі об'єкти, порушення роботи або руйнування яких може спричинити величезні або навіть незворотні негативні наслідки для економіки, добробуту та здоров'я населення, стабільного перебігу політичних процесів [1].

Відповідно до структури преамбули Закону України «Про основні засади забезпечення кібербезпеки України», в ньому закріплюються чотири напрями нормативно-правового регулювання:

1) правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі;

2) основні цілі, напрями та принципи державної політики у сфері кібербезпеки;

3) повноваження державних органів, підприємств, установ, організацій, осіб та громадян у сфері кібербезпеки;

4) основні засади координації їхньої діяльності із забезпечення кібербезпеки.

До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання

електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Найбільшу складність представляє розуміння об'єктів критичної інфраструктури та юридичних критеріїв організації їх кіберзахисту.

Ефективність функціонування сучасних систем та технологій виявлення кібератак (кіберзагроз) істотно залежить від оперативності та достовірності моніторингової інформації про активність кіберзлочинців на попередніх стадіях реалізації атак на інформаційні ресурси, зокрема й критично важливі. Аналіз світового досвіду, на сьогодні, вказує, що найбільш ефективним методологічним підходом до побудови інноваційних інтелектуальних моніторингових систем кібернападів є шлях створення ієрархічних багаторівневих структур розпізнавання кібератак (кіберзагроз) на початкових стадіях їхньої реалізації. При цьому, ієрархічний підхід дає змогу розв'язувати складні задачі управління процесом захисту інформації від кібератак в розподілених критично важливих інформаційних системах як послідовність.

На даній час рівень захисту інформаційних ресурсів України як державних, так і недержавних, у тому числі об'єктів критичної інфраструктури, є таким, що потребує вдосконаленню. Цей прикрий факт не є новиною у середовищі фахівців з інформаційної безпеки України - Ukrainian Information Security Group (UISG). В умовах очукуваної кібер-агресії на інформаційні ресурси України фактично кожний власник інформаційного ресурсу залишається сам-на-сам проти організованого та потужного ворогу. Наприклад, від масованих атак типу DDoS можливо захиститися лише колективно, за допомогою сторонніх anti-DDoS-сервісів. Тому на даній час актуальним є питання створення єдиного довіреного Координаційного Центру обміну інформацією про інциденти інформаційної безпеки. Основною проблемою у даному аспекті є саме достатній рівень довіри до такого Центру, оскільки часто інформація, що надсилатиметься до нього, матиме конфіденційний характер, і яку небажано передавати третім особам. Тут важливим є створення подібної структури за участю власників інформаційних ресурсів усіх форм власності, а також професійної ІБ-спільноти, громадських організацій, бізнесу, державних органів, інших зацікавлених сторін. У світі давно напрацьований досвід зі створення та функціонування подібних організацій під загальною назвою Computer Emergency Response Team (команда реагування ні

інциденти комп'ютерної безпеки), які об'єднані у міжнародну організацію FIRST.

Важкість можливих наслідків за такими показниками:

– вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення);

– економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих);

– екологічна шкода (вплив на населення та навколишнє природне середовище);

– взаємозв'язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури) [3].

Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України «Про захист персональних даних». Зокрема у статті 29 цього акту «Міжнародне співробітництво та передача персональних даних» встановлюється, що:

Співробітництво з іноземними суб'єктами відносин, пов'язаних із персональними даними, регулюється Конституцією України, цим Законом, іншими нормативно-правовими актами та міжнародними договорами України.

Передача персональних даних іноземним суб'єктам відносин, пов'язаних із персональними даними, здійснюється лише за умови забезпечення відповідною державою належного захисту персональних даних у випадках, встановлених законом або міжнародним договором України.

Держави-учасниці Європейського економічного простору, а також держави, які підписали Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, визнаються такими, що забезпечують належний рівень захисту персональних даних.

Кабінет Міністрів України визначає перелік держав, які забезпечують належний захист персональних даних.

Персональні дані не можуть поширюватися з іншою метою, ніж та, з якою вони були зібрані [2].

Не можна стверджувати, що в Україні не приділяється увага захисту важливих об'єктів, систем та ресурсів, які, зазвичай, відносять до критичної інфраструктури. Навпаки, діє низка законодавчих актів, що визначають особливості забезпечення захисту таких об'єктів. Однак, рівень недосконалості категоріального юричного наповнення таких актів сьогодні не відповідає потребам сучасності. Тавтологічність, неструктурованість та інші вади визначень у законодавстві можуть негативно відбитися напрактиці застосування норм про кіберзахист України.

Водночас, в державі досі відсутній загальний механізм управління захистом та безпекою цих об'єктів, спостерігаються непоодинокі випадки дублювання функцій та ресурсів, відсутність спільних підходів та узгодженості дій стосовно проблем національного масштабу, а загрози таким об'єктам розглядаються в суто «відомчому» розрізі.

Процес визначення елементів критичної інфраструктури включає оцінювання ризиків для об'єктів, спричинених факторами різного походження (техногенного, природного та соціально-політичного характеру), аналіз взаємозалежностей між цими елементами. Вказане потребує проведення ґрунтовних наукових досліджень, а також розробки та впровадження відповідних інформаційно-правових технології з подальшим внесенням змін до чинного законодавства України.

Література:

1. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (PATRIOT ACT). URL: http://frwebgate.access.gpo.gov

2. Про захист персональних даних. Закон України. Редакція від 30.01.2018 № 2168-VIII. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.

3. Council Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection». URL: http://eur-lex.europa.eu

DOI https://doi.org/10.30525/978-9934-26-266-1-47

ЗНАЧЕННЯ ПІДРОБКИ ДОКУМЕНТІВ В БЕЗПЕКОВІЙ СФЕРІ ПІД ЧАС ВОЄННОГО СТАНУ

Сокуренко Віталій Валерійович
кандидат юридичних наук,
доцент кафедри кримінального права та кримінології
Одеський державний університет внутрішніх справ
м. Одеса, Україна

На сьогодні наша країна перебуває у найбільш складному становищі з часів проголошення її незалежності внаслідок агресивного повномасштабного російського вторгнення (так званої спеціальної визвольної операції). Ці події призвели не тільки до змін у соціальному, економічному, політичному становищі регіонів, але й до появи нових викликів та зміни акцентів у розподілі злочинності та змін чинного кримінального законодавства. До воєнного вторгнення більш-менш стабільна криміногенна ситуація злочинності наразі характеризується появою нових видів кримінальних правопорушень та трансформацією розповсюджених кримінальних правопорушень.

Особливої актуальності на нашу думку набуває в умовах сьогодення, а саме впровадження на території України воєнного стану, такий вид кримінальних правопорушень як підробка документів. Цей вид протиправної діяльності в умовах війни надзвичайно затребуваний як злочинним світом так і ворогом. Причиною цього є можливість підробки документів з метою перетину кордону або проведення диверсійних дій як громадянами України, так і іноземцями. Саме тому правоохоронні органи, як органи, функцією якого є виявлення та попередження правопорушень, посилили діяльність у напрямку виявлення правопорушень у сфері підробки документів. З цією метою було розміщено блок-пости, метою яких є виявлення адміністративних та кримінальних правопорушень, враховуючи і перевірку документів щодо можливості факту їх підробки.