12. Vedushchii «60 minut» Evhenii Popov obyiasnil, zachem nuzhno obsuzhdat Ukrainu. URL: https://www.vesti.ru/doc.html?id=3196392&tid=105474.
13. Zhuravlev D. Nevypolnenie Ukrainoi minskikh sohlashenii Hermanii kraine nepriiatno. URL: https://ru.armeniasputnik.am/radio/20191001/20612827.html.
14. Yshchenko R. Krome «minskikh dohovorennostei» est plokhoi put resheniia problemy, i ochen plokhoi. URL: https://ru.armeniasputnik.am/radio/20191023/20852000/ ishenko-problema.html.
15. Kosachev K. Podpisanie «formuly Shteinmeiera» – pobeda zdravoho smysla. URL: https://rg.ru/2019/10/ 01/kosachev-podpisanie-formuly-shtajnmajera-pobeda-zdravogo-smysla.html.
16. Na rosiiskomu TB isnuie shist osnovnykh naratyviv, spriamovanykh proty Ukrainy – doslidzhennia UKMTs. URL: https://ms.detector.media/mediaprosvita/research/ na_rosiyskomu_tb_isnue_shist_osnovnikh_narativiv_ spryamovanikh_proti_ukraini_doslidzhennya_ukmts/.
17. Pushylyn D. Zelenskii povtoriaet Poroshenko v samykh khudshykh eho proiavlenykh URL: https://ru.armeniasputnik.am/world/20191025/20870472/Pushilin-Zelenskiy-povtoryaet-Poroshenko-v-samykh-khudshikh-ego-proyavleniyakh.html.
18. Rosiiskyi vplyv na ukrainski media: doslidzhennia. URL: https://ua.ejo-online.eu/2012/mediadoslidzhennia/rosiiskyi-vplyv-na-ukrainski-media.
19. Skabeeva i Popov kak same uspeshnye molodye politicheskie telezhurnalisty. URL: https://tjournal.ru/ news/86986-skabeeva-i-popov-kak-samye-uspeshnye-molodye-politi cheskie-telezhurnalisty.
20. Stavlennia naselennia do ZMI ta spozhyvannia riznykh typiv media u 2019 r. URL: https://detector.media/ infospace/article/171769/2019-10-22-stavlennya-naselennya-do-zmi-ta-spozhivannya-riznikh-tipiv-media-u-2019-r/.
21. Ukraina podpisala «formulu Shtainmaiera». URL: https://lenta.ru/brief/ 2019/10/01/steinmeier/.
22. Ukrainskaia «partiia voiny» poterpela porazhenie v Minske. URL: https://vz.ru/world/2019/10/1/415640.html.
23. Formula rozbratu. URL: https://m.tyzhden.ua/Politics/235795.
24. Tsyfra tyzhnia: 1,3 miliarda. URL: https://www.stopfake.org/uk/tsyfra-tyzhnya-1-3-milyarda/.
25. Chto takoe «formula Shtainmaiera»? URL: https://www.bbc.com/ukrainian/news-russian-49921602.

УДК 351.746:007](4)

Панас Вікторія,
магістр факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі України,
Луцьк, Україна
panas.viktoriya@gmail.com;
Новак Роман,
студент 4-го курсу факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі України,
Луцьк, Україна
Roman.Novak2016@eenu.edu.ua;
Козак Володимир,
студент 4-го курсу факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі України,
Луцьк, Україна
Volodymyr.Kozak2016@eenu.edu.ua

ТЕНДЕНЦІЇ ТА СПЕЦИФІКА ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ В КРАЇНАХ ЄВРОПИ

Інформаційна безпека сучасного суспільства є актуальним питанням вирішення та попередження гібридних загроз як світовій спільності, так і європейським країнам зокрема.
У статті проаналізовано та схарактеризовано тенденції швидкого розвитку інформаційного тероризму та специфіку його протистояння в різних країнах Європи, таких як Сполучене Королівство Великобританії й Північної Ірландії, Німеччини та Франції.
Незмінна система захисту інформаційного простору консервативної Великобританії доводить, що світова спільнота спроможна об'єднатись і виступити проти кібератак, скоєних іншою державою для забезпечення безпеки своїх громадян.

Із метою розробки пропозицій із вироблення стратегії державної політики та контроль виконання рішень керівництва держави у сфері протидії кіберзагрозам у ФРН створено вищий дорадчо-консультативний орган – Національну раду кібербезпеки. Для оптимізації оперативного співробітництва між усіма державними установами й поліпшення координації заходів із протидії кібератакам у ФРН створено Національний центр кіберзахисту у сфері управління Федерального відомства захисту інформаційних систем, який безпосередньо взаємодіє зі спецслужбами та поліцейськими структурами країни, із приватним сектором Німеччини, державами-партнерами з ЄС, НАТО, а також міжнародними організаціями.

У Франції захист державної таємниці на державному рівні здійснюється на основі статей Кримінального кодексу, комерційна таємниця захищається статтями Кримінального кодексу, Трудового й Цивільного кодексу. Франція активно підтримує країни, які висунули проти російських спецслужб звинувачення в кібератаках на міжнародні організації, що перебувають на їхній території.

Сучасні Європейські організаційні структури, що розглядались у дослідженні можуть значно підвищить рівень захищеності від кіберзагроз не лише національного кіберпростору ФРН, а й більшості країн-партнерів Німеччини за рахунок чіткої та оперативної їх взаємодії.

Ключові слова: *інформаційний тероризм, Великобританія, Німеччина, Франція, інформаційний захист, інформаційна безпека, кібербезпека, кібератака.*

1. ВСТУП

Постановка проблеми. Інформаційний тероризм постійно й активно порушує всі засоби безпеки держав світу та зачіпає інтереси як окремої особистості, так суспільства та держави загалом. Застосування терористами новітніх досягнень науки й техніки значно розширює їхні руйнівні можливості. Нині для терористів легко вразливі практично всі комп‟ютерні засоби обробки та зберігання інформації.

Щороку законодавство країн Європи з питань захисту інформації вдосконалюється й дає приклад країнам, що розвиваються, та державам із перехідною економікою, як потрібно розвивати власне національне законодавство, аби досягти успіхів та впевнено ввійти у світовий інформаційний простір.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасними загрозами інформаційній безпеці міжнародного значення є інформаційний тероризм, комп‟ютерна злочинність, інформаційні війні, використання інформаційної зброї, маніпулювання громадською думкою тощо [5].

Зі свого боку, інформаційний тероризм – це злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами задля сприяння здійсненню терористичних операцій або акцій [3].

На сьогодні виокремлюють різні види інформаційного тероризму, серед яких найпоширенішими є медіа-тероризм і кібертероризм. Сутність медіа-тероризму полягає в спробах шляхом організації спеціальних медіа-кампаній дестабілізувати суспільство, створити в ньому атмосферу громадянської непокори, недовіри суспільства до дій, намірів влади й, особливо – її силових структур, покликаних захищати суспільний порядок [6].

З іншого боку, кібертероризм – це сукупність дій, що включають інформаційну атаку на комп‟ютерну інформацію, обчислювальні системи, апаратуру передання даних, інші складники інформаційної інфраструктури, яка скоюється злочинними угрупуваннями або окремими особами.

Щодо країн Європи, то уряд *Великобританії* розпочав роботу над проблемами захисту інформації набагато раніше за інші європейські держави, що й дало їм змогу набути досить корисний досвід у цій сфері. Основною метою було, є та залишається – безпека країни і її громадян. Відповідно до цього, усі державні органи, які захищають інформацію, забезпечують опір дезінформації й стабільність моніторингу правдивості та достовірності контенту, створюються урядом, підпорядковані йому ж або відповідним спецслужбам.

Базис правового забезпечення інформаційного захисту Великобританії – закони «Про державні документи» і «Про державну таємницю». Безпека іншого виду інформації забезпечується кримінальним кодексом та іншими нормативно-правовими актами. Що ж стосується захисту

комерційної таємниці, то кожна організація повинна піклуватися про це самостійно, укладаючи договори з працівниками для надання їм доступу до даних.

Організації, що контролюють сферу інформаційного захисту у ВБ, підпорядковані винятково уряду. Окрім того, великі комерційні компанії мають свої власні служби інформаційної й кібербезпеки. Середній бізнес здебільшого послуговується можливостями та пропозиціями приватних організацій і компаній, що реалізовують, підтримують корпоративні системи захисту інформації. Ці служби часто об‟єднують зусилля й взаємодіють одна з одною та з державними структурами [1].

Правоохоронні й спеціальні структури Великобританії, незважаючи на ґрунтовну нормативно-правову базу, постійно намагаються взаємодіяти з провайдерами. Головною віхою, що тісно взаємодіє з комунікаційними операторами, особливо з питань дозволеного контенту та фільтрації інформації, є Офіс із комунікацій, створений ще у 2003 р.

Основна мета загальної інформаційної стратегії Сполученого королівства полягає в удосконаленні умов конкуренції на інформаційному ринку, зростанні ефективності інформаційних послуг і впровадження інформаційних технологій у державне управління. Особливою рисою інформаційної політики Великобританії є створення регіональних мереж та супермагістралей для оптимізації й підвищення ефективності міжрегіонального та міждержавного науково-технічного співробітництва.

Стійка й чітко контрольована система захисту інформаційного простору у Великобританії залишається незмінною протягом багатьох років. Хоча у 2017 р. зафіксовано зростання кібератак із боку російських хакерів, у тому числі на урядові установи. Зі слів Кіарана Мартіна – голови Центру національної кібербезпеки країни (NCSC), російська агресія в кіберпросторі істотно посилилася, зокрема відзначається зростання кількості кібератак на «незахищені цілі», такі як місцеві ради, благодійні установи та університети, де хакери намагаються добути персональні дані або наукові розробки. Крім того, зловмисники намагаються викрасти із баз даних урядових відомств секретну інформацію, що стосується зовнішньої політики й оборони [9].

За 2018 р. співробітники Центру національної кібербезпеки (NCSC) зафіксували понад 600 серйозних інцидентів. За оцінками британських експертів, наразі спроби російських хакерів не можна назвати успішними [4].

Національний центр кібербезпеки Великобританії (NCSC) встановив, що ГРУ РФ стоїть за більшістю хакерських угруповань, які організували кібератаки в різних країнах світу. Ці кібератаки є грубим порушенням міжнародного законодавства, вони вплинули на життя громадян низки країн і завдали мільйони економічних збитків.

Міністр закордонних справ Великобританії Джеремі Хант заявив: «Ці кібератаки не служать ніяким законним інтересам національної безпеки, вони створюють перешкоди повсякденному житті людей по всьому світу. Наша позиція однозначна: разом з нашими союзниками ми будемо викривати й відповідним чином відповідати на спроби ГРУ підірвати міжнародну стабільність» [2].

Отже, незмінна система захисту інформаційного простору консервативної Великобританії доводить, що світова спільнота спроможна об‟єднатись і виступити проти кібератак, скоєних іншою державою для забезпечення безпеки своїх громадян.

Німеччина – одна з найбільш розвинутих країн Західної Європи в галузі інформаційної безпеки. Ця держава має розвинуту структуру органів, що займаються захистом різних видів інформації з обмеженим доступом. Від самого початку створення цієї системи захисту інформації увагу акцентовано на захист від промислового шпигунства й охорону державних секретів. Характерною особливістю для цієї країни є те, що установи, які вперше займалися окресленими питаннями, почали створюватися ще в XIX ст.

Із середини XX ст. Німеччина багато уваги приділяла захисту такого виду інформації, як персональні дані. У Німеччині захист персональних даних не лише добре визначений законодавством, а й реально забезпечується в практичній діяльності й житті. Німецьке законодавство з питань захисту персональних даних ґрунтується на положеннях, які випливають із принципу інформаційного самовизначення. Тому кожний громадянин сам розпоряджається своїми персональними даними. Якщо в інтересах держави він повинен відкривати цю інформацію, то питання державних установ до нього повинні обмежуватися необхідним мінімумом, наприклад сплата податків. Використання персональних даних громадян у Німеччині суворо заборонене. Звідси випливає, що таку інформацію про своїх жителів дозволяється збирати й використовувати лише в рамках чітко окреслених законом цілей [8].

У Німеччині сформувалися недержавна та державна системи захисту інформації. Недержавну систему захисту інформації покладено на підприємства. Це стосується переважно захисту конфіденційної інформації, пов‟язаної з комерційною таємницею. Захистом держаних секретів займається держава.

Керівництво ФРН, розуміючи загрозу національній безпеці через зростаючі масштаби світової кібернетичної злочинності, приділяє велику увагу державній політиці з мінімізації негативних наслідків такої протиправної діяльності. Крім прийняття законодавчих актів, що регламентують вимоги забезпечення захисту інформації в інформаційно-телекомунікаційних мережах Німеччини, Урядом країни затверджено Стратегію кібернетичної безпеки ФРН, яка є головним доктринальним документом із захисту інформаційної інфраструктури країни від кібернетичних атак. Концепція визначає низку дефініцій у галузі кібернетичної безпеки, кібернетичні загрози інформаційній інфраструктурі, об‟єкти та суб‟єкти посягання, а також організаційні засади протидії протиправним проявам.

Із метою розробки пропозицій із вироблення стратегії державної політики й контроль виконання рішень керівництва держави у сфері протидії кіберзагрозам у ФРН створено вищий дорадчо-консультативний орган – Національну раду кібербезпеки. Для оптимізації оперативного співробітництва між усіма державними установами й поліпшення координації заходів із протидії кібератакам у ФРН створено Національний центр кіберзахисту у сфері управління Федерального відомства захисту інформаційних систем, який безпосередньо взаємодіє зі спецслужбами та поліцейськими структурами країни, із приватним сектором Німеччини, державами-партнерами з ЄС, НАТО, а також міжнародними організаціями.

Така організаційна структура, на думку німецької влади, підвищить рівень захищеності від кіберзагроз не лише національного кіберпростору ФРН, а й більшості країн-партнерів Німеччини за рахунок чіткої та оперативної їх взаємодії [11].

У період із 1 липня 2017 р. до 31 травня 2018 р. отримано 145 повідомлень про кібернапади на німецькі об‟єкти критично важливої інфраструктури. Більшість із них скоєно в ІТ та телекомунікаційному секторі, а також у сфері енергетики. При цьому атаки стають усе більш складними.

За даними Федерального відомства з безпеки у сфері інформаційної техніки (Bundesamt für Sicherheit in der Informationstechnik – BSI), кількість шкідливих програм зросла до 800 млн. Щодня до них додається ще близько 390 тис. нових варіантів. «Відомі сімейства шкідливих програм продовжують змінюватися, доповнюватися та оснащуватися додатковими функціями», – ідеться у звіті BSI. У відомстві також зазначили, що урядові мережі стають мішенню хакерів майже щоденно.

Найчастіше кібернапади здійснюються за допомогою шкідливих програм, які відправляють електронною поштою. BSI повідомило, що за місяць у реальному часі перехоплюється близько 28 тис. електронних листів, перш ніж вони потрапляють до скриньок отримувачів [10].

У *Франції* питання врегулювання безпеки належать до компетенції прем‟єр-міністра. Він видає накази й погоджує заходи щодо забезпечення захисту секретних матеріалів та інформації, що стосується національної оборони й державної безпеки.

Прем‟єр-міністру надає допомогу генеральний секретаріат національної оборони (SGDN), котрий забезпечує організацію та проведення відповідних заходів, спрямованих на захист секретної інформації, а також контроль за їх виконанням.

У цій країні захист державної таємниці здійснюється на основі статей Кримінального кодексу, комерційна таємниця захищається статтями Кримінального кодексу, Трудового й Цивільного кодексу.

Французьке оборонне відомство має намір посилити захист від кібератак. Франція вразлива до кібератак із боку іноземних держав, заявив міністр оборони країни Жан-Ів Ле Дріан. За його словами, лише у 2016 р. служби кібербезпеки відбили 24 000 атак на комп‟ютерні мережі очолюваного ним відомства. Протягом 2016–2019 рр. щорічно кількість кібератак подвоюється, зазначив Ле Дріан. Небезпека загрожує також цивільній інфраструктурі – комп‟ютерним системам електро- й водопостачання, охорони здоров‟я, транспорту, телекомунікацій. Хакерські атаки становлять загрозу також для ЗМІ й усієї французької влади, – наголосив міністр [7].

Міністр оборони зазначив, що до кінця 2020 р. кількість фахівців із кібербезпеки буде подвоєно. Також Франція підтримує країни, які висунули проти російських спецслужб звинувачення в кібератаках на міжнародні організації, що розміщені на їх території.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, результатом дослідження є системний аналіз та характеристика тенденцій швидкого розвитку інформаційного тероризму, а також специфіка його протистоянню в різних країнах Європи, таких як Сполучене королівство Великобританії й Північної Ірландії, Німеччині та Франції.

Як відомо, незмінна й стійка система захисту інформаційного простору консервативної Великобританії доводить, що світова спільнота спроможна об"єднатися та виступити проти постійних і новітніх кібератак, скоєних іншою державою для забезпечення безпеки своїх громадян.

Сучасні європейські організаційні структури, що розглядались у дослідженні, можуть значно підвищить рівень захищеності від кіберзагроз не лише національного кіберпростору ФРН, а й більшості країн-партнерів Німеччини за рахунок чіткої та оперативної їх взаємодії.

Аналізуючи вищесказане зазначимо, що найбільш чітка система органів, які займаються захистом інформації, існує якраз у країнах Європи. У державах діють служби безпеки, котрі займаються захистом інформації в промислових, торговельних фірмах, у сфері оборонної промисловості, приватної служби захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бусол О. Основні риси контролю за національним інформаційним простором Королівства Велика Британія. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2962:osnovni-risi-kontrolyu-za-natsionalnim-informatsijnim-prostorom-korolivstva-velika-britaniya-2&catid=71&Ite mid=382.
2. Великобритания раскрыла совершѐнные Россией кибератаки. URL: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks.ru.
3. Гавриш С. Б. Комп"ютерний тероризм : сучасний стан, прогнози розвитку та шляхи протидії. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2009. № 20.
4. За рік у Великій Британії зафіксували більш ніж 600 кібератак з боку РФ. URL: https://www.5.ua/svit/u-velykii-brytanii-zaiavyly-pro-nevdali-kiberataky-rosiiskoho-hru-pered-otruienniam-skrypaliv-177148.html.
5. Косілова О. І. Інформаційна безпека України в умовах глобалізації. *Правова інформатика.* 2010. № 3 (27). С. 27.
6. Єрохіна Т. Медіа-тероризм серед інших видів тероризму: спроба типологічного аналізу. URL: http://www.social-science.com.ua/article/1002.
7. Міноборони Франції подвоїть кількість фахівців з кібербезпеки. URL: https://www.dw.com/uk/міноборони-франції-подвоїть-кількість-фахівців-з-кібербезпеки/a-37057663-0.
8. Сідак В. Організація системи захисту інформації в Німеччині: еволюція та сучасний стан. *Прав., нормат. та метрол. забезп. системи захисту інформації в Україні.* 2006. Вип. 2. С. 7–11.
9. У Великобританії повідомили про суттєве зростання кіберагресії з боку Росії. URL: https://www.unian.ua/world/1773022-u-velikobritaniji-povidomili-pro-sutteve-zrostannya -kiberagresiji-z-boku-rosiji.html.
10. У Німеччині зростає кількість кібератак на об"єкти інфраструктури. URL: https://www.dw.com/uk/у-німеччині-зростає-кількість-кібератак-на-обєкти-інфраструкту ри/a-45841892-0.
11. Чернухін І. О. Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. *Інформаційна безпека людини, суспільства, держави.* 2014. № 1. С. 27–43.

Матеріал надійшов до редакції 17.12.2019 р.

TENDENCIES AND SPECIFICITY OF INFORMATION TERRORISM IN EUROPEAN COUNTRIES

Information security of modern society is an urgent issue to address and prevent hybrid threats to the world community and European countries in particular.

The article analyzes and characterizes the tendencies of information terrorism rapid development and the specificity of its confrontation in various European countries, such as the United Kingdom of Great Britain and Northern Ireland, Germany and France.

The unchanging system of protection of the information space of conservative Great Britain proves that the world community is able to unite and oppose cyber attacks committed by another state to ensure the safety of its citizens.

In order to develop offers for the development of public policy strategy and control the implementation of decisions of the state leadership in the field of combating cyber threats in Germany, a supreme advisory body – the National Cyber Security Council – was created. To optimize operational cooperation between all government agencies and improve the coordination of measures to combat cyber attacks in Germany, the National Center for Cyber Defense in the field of management of the Federal Office for Information Systems Protection has been established, which interacts directly with the country"s intelligence services and police, with the German private sector, partner countries with the EU, NATO, and international organizations.

In France, the protection of state secrets at the state level is based on the articles of the Criminal Code, trade secrets are protected by articles of the Criminal Code, Labor and Civil Code. France actively supports countries that have accused Russian intelligence services of cyber attacks on international organizations located on their territory.
The current European organizational structures considered in the study can significantly increase the level of protection against cyber threats not only to the national cyberspace of Germany, but also to most of Germany‟s partner countries due to their clear and efficient interaction.
Key words: information terrorism, Great Britain, Germany, France, information protection, information security, cybersecurity, cyber attack.

REFERENCES

1. Busol O. Osnovni rysy kontroliu za natsionalnym informatsiinym prostorom Korolivstva Velyka Brytaniia. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2962:osnovni-risi-kon trolyu-za-natsionalnim-informatsijnim-prostorom-korolivstva-velika-britaniya-2&catid=71&Ite mid=382.
2. Velikobritaniia raskryla sovershonnye Rossiei kiberataki. URL: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks.ru.
3. Havrysh, S. B. Kompiuternyi teroryzm: suchasnyi stan, prohnozy rozvytku ta shliakhy protydii. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka),* 2009, 20.
4. Za rik u Velykii Brytanii zafiksuvaly bilsh nizh 600 kibiratak z boku RF. URL: https://www.5.ua/svit/u-velykii-brytanii-zaiavyly-pro-nevdali-kiberataky-rosiiskoho-hru-pered-otruienniam-skrypaliv-177148.html.
5. Kosilova, O. I. Informatsiina bezpeka Ukrainy v umovakh hlobalizatsii. *Pravova informatyka,* 2010, 3 (27), 27.
6. Yerokhina, T. Media-teroryzm sered inshykh vydiv teroryzmu: sproba typolohichnoho analizu. URL: http://www.social-science.com.ua/article/1002.
7. Minoborony Frantsii podvoit kilkist fakhivtsiv z kiberbezpeky. URL: https://www.dw.com/uk/minoborony-frantsii-podvoit-kilkist-fakhivtsiv-z-kiberbezpeky/a-37057663-0.
8. Sidak V. Orhanizatsiia systemy zakhystu informatsii v Nimechchyni: evoliutsiia ta suchasnyi stan. *Prav., normat. ta metrol. zabezp. systemy zakhystu informatsii v Ukraini,* 2006, 2, 7–11.
9. U Velykobrytanii povidomyly pro suttieve zrostannia kiberahresii z boku Rosii. URL: https://www.unian.ua/ world/1773022-u-velikobritaniji-povidomili-pro-sutteve-zrostannya -kiberagresiji-z-boku-rosiji.html.
10. U Nimechchyni zrostaie kilkist kiberatak na obiekty infrastruktury. URL: https://www.dw.com/uk/u-nimechchyni-zrostaie-kilkist-kiberatak-na-obiekty-infrastruktu ry/a-45841892-0.
11. Chernukhin, I. O. Dosvid Federatyvnoi Respubliky Nimechchyny v pobudovi systemy zakhystu infrastruktury vid kibernetychnykh zahroz. *Informatsiina bezpeka liudyny, suspilstva, derzhavy,* 2014, 1, 27–43.

UDK 351.746:007](8=134)
Piskors'ka Yuliia,
4th year student of Faculty of International Relations
Lesya Ukrainka Eastern European National University,
Lutsk, Ukraine
Yuliia.Piskorska2016@eenu.edu.ua;
Burda Anna,
4th year student of Faculty of International Relations
Lesya Ukrainka Eastern European National University,
Lutsk, Ukraine
Anna.Burda2016@eenu.edu.ua;
Roshko Ivan,
4th year student of
Faculty of International Relations
Lesya Ukrainka Eastern European National University,
Lutsk, Ukraine
Ivan.Roshko2016@eenu.edu.ua

INFORMATION SECURITY IN LATIN AMERICA

Many Latin American companies are not ready to protect their data and are falling behind their international colleagues in terms of cyber insurance adoption. Cybercrime imposes a huge threat for their economies. The states