

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ
МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ**

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

ІХ Всеукраїнська науково-практична конференція

**Збірник тез наукових доповідей
(Київ, 30 березня 2018 року)**

Електронна версія

Київ
2018

Організаційний комітет конференції:

Кудінов С.С. – голова організаційного комітету конференції, ректор Національної академії СБ України, кандидат юридичних наук, доцент; **Золотухін Д.Ю.** – співголова, заступник Міністра інформаційної політики України; **Пилипчук В.Г.** – співголова, директор Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України; **Спірін О.М.** – співголова, в.о. директора Інституту модернізації змісту освіти Міністерства освіти і науки України, доктор педагогічних наук, професор; **Фальченко С.Л.** – проректор з наукової роботи Національної академії Служби безпеки України, кандидат юридичних наук, доцент; **Довгань О.Д.** – перший заступник директора Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, старший науковий співробітник; **Чорний Р.Л.** – директор науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук, старший науковий співробітник; **Мамченко С.М.** – директор Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор педагогічних наук, професор; **Муратов О.Є.** – заступник директора центру – начальник організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник; **Панченко В.М.** – заступник директора інституту (з навчальної і наукової роботи) Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник; **Дашковська О.В.** – старший науковий співробітник відділу модернізації вищої освіти Інституту модернізації змісту освіти Міністерства освіти і науки України, кандидат хімічних наук, доцент; **Макобрій О.О.** – головний спеціаліст сектору стратегічних комунікацій Міністерства інформаційної політики України; **Давидова Т.О.** – старший науковий консультант організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук

Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – Київ : Нац. акад. СБУ, 2018. – 408 с.

У збірнику висвітлюються актуальні проблеми забезпечення інформаційної та кібернетичної безпеки України та науково-практичні підходи до їх вирішення. Розглядаються питання формування системи забезпечення кібернетичної безпеки України, розвитку стратегічних комунікацій в Україні, удосконалення вітчизняного законодавства у сфері охорони державної та службової інформації, шляхи оновлення змісту вищої освіти фахівців з інформаційної безпеки держави.

Для працівників органів державної влади, науковців, викладачів, фахівців з інформаційної безпеки, широкої громадськості.

Тези доповідей публікуються в авторській редакції. Організаційний комітет залишає за собою право не поділяти думку авторів.

певні засоби захисту інформації, а також визначити основні пріоритети витрачання коштів, передбачених у бюджеті на забезпечення інформаційної безпеки (якщо підприємство практикує виділення фіксованих сум на ці цілі).

Література

1. Анисимов А.А. Менеджмент в сфере информационной безопасности М.: БИНОМ, 2009.
2. Основы управления информационной безопасностью / А.П.Курило, Н.Г.Милославская, М. Ю.Сенаторов и др. – М.: Горячая линия-Телеком, 2012.
3. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи, ДМК-Пресс, 2004.
4. Артемов В.Ю. Основы менеджменту для інформаційних аналітиків: курс лекцій / В.Ю.Артемов. – К.: КНТ, 2007.

УДК 004.56

Гулак Г.М.

кандидат технічних наук, доцент
Національна академія СБ України

Кащук В.І.

Національна академія СБ України

Складанний П.М.

Київський університет ім. Б. Грінченко

УТОЧНЕНА МОДЕЛЬ ПОРУШНИКА ТА МОДЕЛЬ РЕАЛІЗАЦІЇ КІБЕРАТАК В СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Реалізація ефективного кіберзахисту (включаючи, криптографічний захисту інформації (КЗІ)), в системах управління технологічними процесами (СУТП) потребує побудови адекватної моделі загроз, що в умовах постійного вдосконалення методів та засобів нападу [1] вимагає постійного уточнення моделі потенційного порушника системи захисту [2].

Аналіз повідомлень про кібератаки дає змогу визначити мету його злочинних дій, а саме нанесення суттєвих збитків власнику системи, мінімізуючи при цьому власні фінансові, матеріальні та інші витрати. Для цього, по-перше, він має достатньо високу кваліфікацію та необхідний фінансовий ресурс, технічне і програмне оснащення, які дозволяють йому створювати складні програмні комплекси для реалізації кібератак.

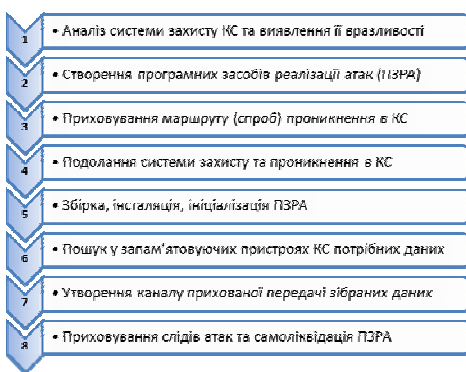
По-друге, згідно з принципом Керкхофса, він знає алгоритми функціонування засобів захисту, включаючи засоби КЗІ, але до початку атаки не знає діючих ключів. По-третє, для досягнення поставлених цілей порушник має можливість перехоплення будь якої інформації у транспортній мережі, модифікацію або створення неприпустимої команди за відносно невеликий час.

Виходячи з викладеного, можливо передбачити наступні варіанти його зловмисних дій (потенційних загроз) стосовно СУТП в цілому: 1) модифікація дійсної команди або реальної інформації про внутрішній стан системи; 2) формування та надсилання керованому об'єкту неприпустимої команди або фальшивих даних про внутрішній стан СУТП; 3) перехоплення в транспортній мережі окремих команд або частки інформації щодо внутрішніх станів задля їх вилучення; 4) крадіжка конфіденційної інформації щодо сервісів, які надаються; 5) модифікація або руйнування програмного коду СУТП.

Щодо програмних реалізацій засобів КЗІ, які використовуються в СУТП, можливо вважати, що метою дій порушника може бути: 1) зміна, знищення або крадіжка критичних параметрів CSP; 2) модифікація програмного коду (криптосхеми) засобу КЗІ.

На підставі аналізу наукових публікацій щодо реалізації кібератак у поєднанні з відомими методами криптоаналізу на основі побічних каналів [3] була сформована наступна модель кібератак в СУТП, яка включає вісім фаз активних дій порушника (рис.):

1. Розвідка. На першому етапі порушник, використовуючи всі доступні



методи, здійснює приховане вивчення вразливостей комп'ютерної системи (КС), яка є технологічною базою функціонування СУТП, а також виявлення слабких місць наявної системи захисту [4].

2. Розробка. На цьому кроці, здійснюється вивчення отриманої інформації та розробка програмних засобів для реалізації атак (ПЗРА).

3. Маскування. Порушник здійснює заходи щодо усунення ознак, які пов'язують ПЗРА та спосіб його застосування з реальним розробником, та/або створює фіктивні ознаки, що ототожнюються з непричетними до кібератаки суб'єктами. Також він визначає тактику приховування реального маршруту (адрес проміжних вузлів глобальної мережі) спроб проникнення в КС.

4. Проникнення. Використовуючи створені засоби і технології, а також можливості інсайдерського впливу порушник забезпечує подолання системи захисту та проникнення ядра ПЗРА в програмне середовище КС.

5. Підготовка. Далі в автоматичному або автоматизованому режимі реалізується збирання ПЗРА з окремих модулів, його інсталяція та ініціалізація.

6. Реалізація. Ініціалізоване ПЗРА на основі певної апріорної інформації про підсистеми (елементи) КС, що виконують конкретні функції СУТП, а також про потрібні порушнику дані, зокрема, чутливі параметри безпеки криптографічних модулів SSP виявляє та ідентифікує зазначені об'єкти у запам'ятовуючих пристроях КС. У якості відповідної апріорної інформації можуть виступати розмір файлів, формати даних, певні ключові слова, програмні переривання/звернення до деяких ресурсів системи тощо. Залежно від цілей кібератаки виявлені ресурси можуть бути знищені, модифіковані або використані для розкриття конфіденційної інформації.

7. Витік. За необхідності, створюється канал прихованої передачі зібраних даних з використанням методів стеганографії, процедури стискання даних з наступним шифруванням, фізичного переносу під час підключення зовнішніх пристроїв тощо.

8. Самоліквідація. На завершальному етапі ПЗРА включає механізми самознищення та приховування слідів кібератаки. Цей етап реалізується автоматично, в разі настання в КС певних обставин (наприклад, визначеного часу), або автоматизовано на підставі отримання команди ззовні.

Література

1. Бурячок В.Л. Завдання форми та способи ведення воєн у кібернетичному просторі / В.Л.Бурячок, Г.М.Гулак, В.О.Хорошко // Науково-технічний журнал «Наука та оборона», 2011. – № 3. – С. 35-42.

2. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, в редакції Наказу Адміністрації ДССЗЗІ від 14.12.2015 № 767.

3. J. Kelsey Side Channel Cryptanalysis of Product Ciphers / J. Kelsey, B. Schneier, D. Wagner, C. Hall // 5th European Symposium on Research in Computer Security Louvain-la-Neuve, Belgium September 16–18, 1998 Proceedings, Berlin, Springer, 1998, 97-111 pp.

4. Гулак Г.М. Забезпечення безпеки засобів КЗІ у кіберпросторі / Г.М.Гулак // Матеріали науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» – Т. ІУ Сучасні технології інформаційної безпеки. – К., 2015. – С. 100-102.

ЗМІСТ

ВСТУПНЕ СЛОВО	3
----------------------------	---

ДЕРЖАВНО-ПРАВОВІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Автушенко О.С., Дяченко С.В. Розвиток та перспективи використання IP-телефонії	5
---	---

Анпілогов С.С., Волошин А.Л. Підходи до захисту Android-пристроїв в сучасних інформаційно-телекомунікаційних системах державних органів України від зловмисного програмного забезпечення	7
---	---

Баланда А.Л. Інформаційний обмін як базовий компонент забезпечення міжнародної економічної безпеки	9
---	---

Белай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід’ємна складова воєнної безпеки	12
---	----

Беляков К.І. Законодавство в секторі інформаційної безпеки: технологічно-правовий аналіз	14
---	----

Благодарний А.М. Удосконалення інформаційного забезпечення адміністративно-юрисдикційної діяльності органів СБ України	19
---	----

Богущ В.М. Результати дослідження підходів до реалізації стандарту вищої освіти за спеціальністю «кібербезпека» у сфері підготовки фахівців для національної системи кібербезпеки	21
--	----

Бурій С.В. Значення формування інформаційної культури майбутнього офіцера в процесі навчання як чинника управління інформаційною безпекою держави	25
--	----

Бутвін Б.Л., Гвоздь В.І., Штифурак Ю.М. Методичний підхід до визначення інтегрального рівня зовнішніх загроз кібербезпеці держави на основі нелінійного, параметричного методу їх оцінювання	27
---	----

Буяло О.В., Пилипчук В.В. Один із шляхів вирішення проблеми забезпечення безпеки Web-додатків	30
--	----

Ватраль А.В. Роль контррозвідального пізнання у забезпеченні інформаційної безпеки України.....	31
Вацлавик О.М. Підвищення обізнаності про кібернетичну безпеку.....	33
Величко М.В. Інформаційна безпека біомедичних досліджень: міжнародна політика.....	35
Воскобойніков С.О., Кашук В.І. Формування професійної компетентності сучасного фахівця з кібербезпеки для реалізації компетенцій комп'ютерної криміналістики	38
Гавловський В.Д. До питання налагодження міжвідомчого обміну інформацією.....	40
Головко О.М. Четверте покоління прав людини: безпековий аспект	42
Гордієнко С.Б., Скубак О.М. Завдання аналізу доцільності реалізації заходів щодо забезпечення інформаційної безпеки.....	45
Гулак Г.М., Кашук В.І., Складанний П.М. Уточнена модель порушника та модель реалізації кібератак в системах управління технологічними процесами	47
Гуцалюк М.В. Актуальні питання забезпечення кібербезпеки України.....	50
Гущин О.О. До питання правового регулювання кібероперацій.....	52
Дмитренко Е.С. Актуальні питання забезпечення інформаційної безпеки сфери публічної фінансової діяльності	55
Дмитренко Ю.П. Соціально-правові проблеми комплектування підрозділів суб'єктів забезпечення інформаційної і кібернетичної безпеки та шляхи їх вирішення.....	57
Довгань О.Д. Щодо деяких правових аспектів культури кібербезпеки	60
Доронін І.М. Правові проблеми визначення компетенції суб'єктів забезпечення кібербезпеки України	62

Дралюк І.М. Внутрішні загрози безпеці державного управління України	64
Єрменчук О.П. Інформаційно-комунікаційна складова державно-приватного партнерства у захисті критичної інфраструктури як важливий елемент забезпечення державної безпеки.....	68
Жиляєв І.Б., Семенченко А.І. Організаційно-правове забезпечення розвитку національної системи кібербезпеки України: стан та перспективи	70
Заєць П.М., Іванова О.С. Визначення підходів щодо впровадження засобів і систем автоматизації процесів управління інформаційною безпекою організації.....	72
Зибін С.В. Підтримка прийняття рішень при формуванні програм інформаційної безпеки держави: розподілення ресурсів	75
Золотухін Д.Ю. Боротьба із «фейковими новинами»: досвід України та рекомендації	78
Карпенко О.В., Савченко Н.В. Цифрові технологічні тренди сфери інформаційної безпеки України.....	83
Касперський І.П. Розвиток можливостей ідентифікації та автентифікації користувачів сервісів електронного урядування	85
Кожедуб Ю.В., Прокудо Р.М. До питання створення комплексу заходів із забезпечення безпеки інформації на організаційному рівні.....	88
Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Стратегічні напрямки анкетування спеціалістів інформаційної та кібернетичної безпеки для з'ясування рівня кібернетичної захищеності організації.....	89
Козюра В.Д., Хорошко В.О. Заходи протидії прихованої передачі інформації в локальних мережах	91
Комісаров О.Г. Питання інформаційної безпеки у місцях, якими переміщуються особи.....	93

Корченко О.Г., Дрейс Ю.О., Романенко О.О. Класифікація об'єктів критичної інформаційної інфраструктури держави.....	95
Косик В.М., Мельник О.М. Безпека дітей в Інтернеті як елемент цифрової грамотності	98
Косошов О.М., Сірик А.О. Підхід до моделювання ризиків інформаційній безпеці державної установи.....	100
Костенко О.В. Компрометація особистого ключа електронного підпису (правовий аспект).....	102
Левченко О.В. Методологічний інструментарій оцінювання ефективності системи забезпечення інформаційної безпеки	105
Лісовська О.Л., Ничитайло І.М. Державно-приватне партнерство у сфері забезпечення інформаційної безпеки держави.....	107
Марічев В.Є. Забезпечення СБ України інформаційної безпеки в системі територіальної оборони України.....	109
Мельник Д. С. Щодо актуальних потреб захисту національної критичної інформаційної інфраструктури України.....	112
Мельник С.В. Формування культури кібербезпеки: особистісний, корпоративний, державний та глобальний вимір.....	115
Нізовцев Ю.Ю. Щодо окремих проблем уніфікації понятійно-термінологічного апарату кібербезпеки	118
Ожеван М.А. Публічно-приватне партнерство у кібербезпековій сфері як модернізаційний виклик	120
Пальчик М.Л. Правовий режим інформації про об'єкти критичної інфраструктури.....	124
Панченко В.М. Загрози національній безпеці України в умовах впровадження BigData-технологій	127
Петров В.В. Щодо удосконалення вітчизняного законодавства у сфері кібербезпеки	131

Полотай О.І, Полотай Б.Я. Аналіз порушників та загроз інформаційної безпеки об'єктів готельно-ресторанного господарства	133
Прощасєв В.В. Інформаційна безпека у діяльності зовнішньої розвідки за законодавством Російської Федерації	136
Рижиков В.С. Класифікація загроз інформаційній безпеці, життєво важливі фактори держави в інформаційній сфері	138
Савченко Д.С. До проблем автоматизованого пошуку в неструктурованих текстах в контексті забезпечення інформаційної безпеки.....	140
Самойленко О.О., Кащук В.І. Mobile Technologies у процесі підготовки майбутніх фахівців з інформаційної та кібернетичної безпеки	143
Саричев Ю.О., Хоменко Л.В. Сутність інформаційно-аналітичного забезпечення в системі державного управління у воєнній сфері.....	145
Сафонов Ю.М., Дашковська О.В., Погребняк В.П. Підготовка фахівців у сфері кіберзахисту – пріоритети держави.....	147
Скіцько О.І., Павлючук С.О. Вплив тіньових інформаційних технологій на інформаційну безпеку держави	150
Сніцаренко П.М. Державна інформаційна політика та інформаційна безпека України:щодо сутності і взаємозв'язку	153
Спірін О.М., Юдін.О.К. Концептуальні питання професійної сертифікації фахівців з інформаційної та кібербезпеки в Україні.....	156
Тиква В.Л. Класифікація деструктивної діяльності хакерів	158
Ткачов І.В. Щодо удосконалення концептуальних засад протидії тероризму в Україні: інформаційний аспект	161
Ткачук Н.А. До проблеми формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.....	163

Ткачук Н.І. Національні конституційні та міжнародні норми про інформаційні права людини	165
Ткачук Т.Ю. Аксіологічні константи інформаційної безпеки держави	167
Толюпа С.В., Браїловський М.М. Проблеми підготовки фахівців по кібербезпеці та захисту інформації	169
Уліч В.Л. Технології інформаційної безпеки освітнього процесу у вищих військових навчальних закладах.....	172
Устименко О.В. Мережа ситуаційних центрів сектору безпеки і оборони як єдиний організаційно-технічний комплекс в умовах кризового реагування у сфері оборони	174
Фесенко А.О., Оксіюк О.Г. Проблеми забезпечення інформаційної безпеки безпілотних авіаційних систем	176
Хлань В.Г., Драчук С.М. Сучасні аспекти розвитку європейської та американської ініціатив СБРN в Україні в контексті міжнародної взаємодії у сфері забезпечення інформаційної безпеки	179
Хом'яков Д.О. Нормативно-правове регулювання інформаційної безпеки України	182
Черних Ю.О., Черних О.Б. Таксономія Блума як основний засіб формування компетенцій фахівця з інформаційної безпеки.....	184
Шевченко А.С. Механізми виявлення кібернетичних атак на основі контрольних карт Шухарта	186
Шепета О.В. Забезпечення інформаційної безпеки на підприємстві	188
Штонда Р.М., Паламарчук Н.А., Островський С.М. Соціальні мережі в інтернеті як інструмент загрози національній системі кібербезпеки України.....	190
Щербина Л.І. Суб'єкти забезпечення національної безпеки в інформаційній сфері.....	192
Юрх Н.Г., Блавацька Н.М., Шваб В.К. Маскування мовних повідомлень	195

РОЗВИТОК СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЯК ПЕРЕДУМОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Аблазов І.В., Рубель К.В. Актуальні проблеми дослідження стратегічних комунікацій у війсьній сфері в контексті завдань міністерства оборони України щодо їх реалізації.....	197
Авдошин І.В. Інформаційний простір як об'єкт російської агресії проти України.....	199
Бровко В.Д. Визначення моменту розладки інформаційного потоку	202
Давиденко М.О. Особливості здійснення інформаційно-підривної діяльності з використанням релігійних структур.....	204
Даниленко В.М. Росія і світ: інформаційні загрози і засоби протидії.....	206
Дудатьєв А.В. Концептуальні та науково-методологічні основи захисту держави від деструктивних інформаційних впливів.....	209
Єсімов С.С. Діяльність Національної поліції з забезпечення інформаційної безпеки у контексті діяльності засобів масової інформації	211
Зоренко Д.С. Концепція стратегічних комунікацій в контексті реформування СБ України	213
Іванов О.Ю. Спеціальні інформаційні операції як метод діяльності РФ із псевдолегітимації анексії Автономної Республіки Крим	215
Капосльоз Г.В. Еволюція механізмів інформаційної взаємодії держави й громадян в галузі безпеки та оборони	217
Кожедуб О.В. Мережні війни як різновид інформаційних війн.....	221
Косілова О.І. Сепаратизм в Україні: інформаційна та соціально-політична складова	223
Котляренко О.П. Розвиток стратегічних комунікацій у війсьній сфері	225

Крисяк П.В. Інформаційно-пропагандистський вплив Російської Федерації на населення іноземних країн (на прикладі роботи «фабрики тролів»).....	228
Кубявка Л.Б., Кубявка М.Б. Про вплив, який змінює і повідомлення, і його зміст.....	230
Кухарська Н.П. Проблеми особистісної ідентифікації в інтернет-середовищі.....	231
Лоза В.М., Лалетін С.П., Дяченко І.М. Визначення тональності текстової інформації з використанням методу штучних нейронних мереж в задачі виявлення інформаційно-психологічних впливів	233
Марутян Р.Р. Стратегічні комунікації: поняття, цілі, завдання	235
Марущак А.І. Щодо протидії використанню Інтернет-ресурсів для поширення антиукраїнської інформації	238
Міхєєв Ю.І. Автоматизація оцінювання пропаганди держави-агресора	240
Мокляк С.П. Аналіз існуючої практики підготовки та ведення інформаційного протиборства у сфері військово-технічного співробітництва України	241
Нікіфоров М.М., Жогіна Л.В., Доброгурська О.Б., Нікіфорова О.М. Обґрунтування вибору раціонального алгоритму аналізу тональності різномовної текстової інформації для задачі моніторингу інформаційного простору.....	244
Охрамович М.М., Шевченко В.В., Кравченко О.І. Особливості моніторингу радіо-простору на базі SDR-технології.....	246
Партоленко І.В. Інформаційно-психологічний вплив в контексті інформаційної безпеки держави	249
Петряєв О.С. Ісламський міграційний чинник як стратегічний виклик ціннісно-смісловій безпеці європейських країн	251
Печериця С.В. Зв'язок із засобами масової інформації під час проведення антитерористичної операції	254

Пилипчук В.Г. Інформаційна сфера як складова гібридної війни	256
Покровська А.В. Когнітивна стійкість в контексті протидії терористичній загрозі	260
Прозоров А.Ю. Правове регулювання протидії поширенню негативного контенту екстремістського характеру в інформаційному просторі	262
Радейко Р.І. Блокування інтернет-контенту в механізмі забезпечення національної безпеки	265
Сніцаренко П.М., Саричев Ю.О., Ткаченко В.А., Грицюк В.В. Підсистема моніторингу інформаційного простору як необхідна складова системи протидії негативному інформаційному впливу на особовий склад військ (сил)	267
Соколіна О.В. До питання гібридної війни	270
Соловйов С.Г. Невербальні наративи у стратегічних комунікаціях	272
Ступницька О.І. Психологічні аспекти взаємодії у віртуальних соціальних мережах, інтернет-залежність та її симптоми	274
Тугарова О.К. Недосконалість правового регулювання реклами як деструктивний фактор інформаційної безпеки	276
Хаба Р.С. Деструктивні інформаційні впливи в сучасних реаліях	279
Чередниченко О.Ю. Актуальність осучаснення системи комплексного захисту інформаційних ресурсів національного залізничного перевізника -ПАТ «Укрзалізниця»	281
Черняк А.М. Актуальні питання захисту інформаційного простору	283
Чеховська М.М. Задоволення потреб підприємств і організацій у доступі до інформації як елемент забезпечення інформаційної безпеки держави	285

УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО

Богомолів О.О. Автоматизація режимно-секретної діяльності та управління доступом до інформаційних ресурсів	287
Болдир С.В. Адаптування вимог забезпечення режиму секретності до умов ведення воєнних (бойових) дій з урахуванням досвіду проведення АТО	289
Бондаренко І.Д. Напрямки удосконалення кримінального законодавства у сфері охорони державної таємниці.....	291
Ботвінкін О.В. Організаційне забезпечення захисту секретної інформації органами держбезпеки на території України (друга половина ХХ століття)	294
Гоц О.В. Проблемні аспекти захисту банківської таємниці в Україні	296
Гуз А.М. Окремі питання охорони державної таємниці в Латвійській Республіці	298
Жевелєва І.С. Перспективи взаємодії державного і недержавного секторів безпеки у процесі захисту інформації з обмеженим доступом.	300
Жердєв М.К., Пампуха І.В., Пусан В.В. Мобільні пристрої криптографічного перетворення цифрової інформації.....	302
Князєв С.О. Визначення можливих шляхів підвищення ефективності діяльності працівників режимно-секретних органів	304
Козлова А.О. Актуальні питання запобігання захисту інформації з обмеженим доступом, що циркулює в інформаційних ресурсах туристичних підприємств.....	306
Корченко О.Г., Дрейс Ю.О., Романенко О.О. Формування множини параметрів оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави.....	309

Лебедєв О.Р. Забезпечення охорони державної таємниці у військових умовах у контексті боротьби з ініціативним шпигунством.....	311
Меленті Є.О., Гарбузов О.А., Пономарьов В.О. Удосконалення комплексу технічного захисту інформації об'єктів військового управління.....	313
Мікуліна М.М. Щодо відповідності принципів захисту фізичних осіб при обробці персональних даних	314
Настрадін В.П., Горєлова В.Ю. Розвідка в інформаційному просторі: правові межі.....	318
Попутніков В.Б. Актуальні проблеми законодавчого регулювання охорони державної таємниці при використанні конфіденційного співробітництва	320
Розвадовський О.Б. Державна політика щодо забезпечення охорони державної таємниці та службової інформації у сучасних умовах	323
Рябцова Л.П. Нормативне забезпечення питань охорони інформації, обмін якою здійснюється в рамках співробітництва України з НАТО ...	324
Сидоренко С.М. Організаційно-правові засади охорони державної таємниці Естонської Республіки	327
ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ УЧЕНИХ І СТУДЕНТІВ	
Алєйников І.В. До проблеми інформаційної безпеки держави у воєнній сфері	330
Бараннік В.В. Діяльність органів національного самоврядування кримськотатарського народу як об'єкт інформаційного впливу радянської Росії (1917-1928 рр.): історико-правовий аналіз	332
Білан М.В., Тугарова О.К. Основні напрями реформування інформаційного законодавства України	336
Богдан Д.М. Пошук ефективних шляхів протидії інформаційній агресії РФ щодо України	338

Бондарчук Б.О., Гоц О.В. Управління інформаційними ресурсами Книжкової палати України імені Івана Федорова.....	341
Гаврилюк К.І. Поняття та роль стратегічних комунікацій у сфері публічної дипломатії США	343
Давидюк А.В., Петрик В.М. Протидія автоматизованим засобам використання соціальної інженерії.....	346
Даценко А.Ю. Боротьба з російською дезінформацією як напрям захисту інформаційного простору України в умовах «гібридної війни»	348
Думанська В.О. Недосконалість нормативно-правової бази у сфері кібербезпеки	351
Душкевич В.С. Роль пропагандистської діяльності в інституціалізації Першого Курултаю кримськотатарського народу (грудень 1917 р. – січень 1918 р.): історико-правовий аналіз	353
Коваль М. О., Шуліка В.І. Інформаційна складова сучасних збройних конфліктів	355
Корнійчук М.О., Семчишина С.В. Шляхи оптимізації захисту інформації в Україні	357
Люля В.С., Присяжнюк М.М. Нелінійні та проксі-війни сучасності.....	360
Малоокій Я.М. Проблеми нормативно-правового врегулювання сфери кібербезпеки України та шляхи вирішення цих проблем.....	362
Мовчан А.Ю., Слюсарчук І. В. Залучення особи до виконання завдань правоохоронних органів шляхом комунікативного впливу	363
Осьмак А.С. Перспективи розвитку стратегічної комунікаційної складової публічного врядування в умовах цифровізації суспільства....	366
Преловський К.В. Інформаційна безпека як одна із складових належного функціонування критичної інфраструктури банківської системи України.....	368
Пуркар Д.П., Шепета О.В. Соціальне значення діяльності преси у сфері правового інформування громадян	370

Рагнєв А.О. Використання сучасних феноменів сприйняття інформації як ефективних важелів впливу на свідомість людини.....	373
Роллер В.М. Дотримання принципу пропорційності при здійсненні заходів протистояння російській пропаганді.....	375
Романова Т.В., Гулак Г.М., Кашук В.І. Розвиток технологій криптовалют та їх вплив на здійснення правоохоронної діяльності	377
Саган О.В. Соціальні мережі як інструмент інформаційної війни	379
Селіна М.Б. Стратегічні комунікації як умова реалізації національних інтересів у сфері інформаційної безпеки	381
Сіренко Г.Г. Особливості організації підбору та підготовки кадрів підрозділів кіберзахисту органів публічної влади в сучасних умовах функціонування інформаційного простору України	384
Сорока С.А. Становлення та розвиток нормативно-правового регулювання сфери кібербезпеки в Україні.....	386
Тарасюк А.В. Використання методу профайлінгу співробітниками правоохоронних органів для вирішення проблем у сфері забезпечення інформаційної безпеки держави	389
Фецан В.В., Тугарова О.К. Сутність, напрями та завдання інформаційної політики	391
Щербина Д.С. Підготовка фахівців як проблема у сфері безпеки інформації держави.....	393

Наукове видання

**АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ
ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ**

ІХ Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 30 березня 2018 року)

Електронна версія

Авторська редакція

Технічне редагування, макетування *Т. О. Коркач*

Формат 60x84/16.
Ум. друк. арк. 24,03. Обл.-вид. арк. 23,71.

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. М. Максимовича, 22, Київ, 03022
факс: (044)257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб'єкта видавничої справи ДК № 99 від 23.06.2000