АКАДЕМІЯ ВОЄННО-ПОЛІТИЧНИХ НАУК УКРАЇНИ

Лисецький Ю. М.

КІБЕРБЕЗПЕКА: ВИКЛИКИ, ЗАГРОЗИ, ПРОТИДІЯ

Монографія

Київ 2026

УДК 004.056.5
Л63

Рекомендовано до друку
Вченою радою Академії воєнно-політичних наук України
(протокол № 2 від 06.01.2026 р.)

Лисецький Ю. М. – доктор технічних наук, доцент.

Рецензенти:

Козловський В. В. – доктор технічних наук, професор, завідувач кафедри технічного захисту інформації факультету комп'ютерних наук та технологій Державного університету «Київський авіаційний інститут»;

Легомінова С. В. – доктор економічних наук, професор, завідувач кафедри управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій.

Лисецький Ю. М.

Л63 Кібербезпека: виклики, загрози, протидія: монографія. – Київ : Видавець Бихун В. Ю., 2026. 196 с.

ISBN 978-617-8553-02-9

Монографія присвячена проблемі забезпечення кібербезпеки держави. У дослідженні висвітлено глобальні виклики та загрози в кіберпросторі. Розглянуто сутнісні характеристики формування механізму міжнародної кібербезпеки. Запропоновано концептуальні засади побудови національної системи кібербезпеки, модель системи національної кібербезпеки й модель взаємодії та обміну інформацією між центрами протидії кіберзагрозам. Проаналізовано можливості використання перспективних технологій у кібербезпеці, зокрема квантових, біометричних та штучного інтелекту. Наведено існуючі підходи, методи і способи забезпечення інформаційної та кібербезпеки. Розроблено корпоративну систему інформаційної та кібербезпеки, а також сучасні інструментальні засоби протидії кіберзагрозам – операційну систему кібербезпеки і центр оперативного реагування на кіберінциденти.

Монографія розрахована на науковців, викладачів та аспірантів вищих навчальних закладів, військових і цивільних фахівців, діяльність яких пов'язана з кібербезпекою держави.

ISBN 978-617-8553-02-9

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ

БД	–	бази даних
ВРУ	–	Верховна Рада України
ГРУ	–	Головне розвідувальне управління ЗС рф
ГУР	–	Головне управління розвідки МО України
ГЦЦК	–	Галузевий центр цифровізації та кібербезпеки
ГШ	–	Генеральний штаб
ДНК	–	дезоксирибонуклеїнова кислота
ДСНС	–	Державна служба з надзвичайних ситуацій
ДССЗЗІ	–	Державна служба спеціального зв'язку та захисту інформації України
ЄС	–	Європейський Союз
ЗМІ	–	засоби масової інформації
ЗСУ	–	Збройні Сили України
ІС	–	інформаційна система
КІС	–	корпоративна інформаційна система
КСЗІ	–	комплексна система захисту інформації
КСІК	–	корпоративна система інформаційної та кібербезпеки
МВС	–	Міністерство внутрішніх справ України
МЗС	–	Міністерство закордонних справ України
Мінцифри	–	Міністерство цифрової трансформації України
ММЕ	–	міжмережевий екран
МОУ	–	Міністерство оборони України
НБУ	–	Національний банк України
НД ТЗІ	–	нормативні документи в галузі технічного захисту інформації
ОБСЄ	–	Організація з безпеки і співробітництва в Європі
ООН	–	Організація Об'єднаних Націй
ОС	–	операційна система
ОСК	–	операційна система кібербезпеки
ПАК	–	програмно-апаратний комплекс
ПЗ	–	програмне забезпечення

ПК	–	персональний комп'ютер
РНБО	–	Рада національної безпеки та оборони
рф	–	російська федерація
СБУ	–	Служба безпеки України
СЗД	–	система зберігання даних
СЗР	–	Служба зовнішньої розвідки
СУБД	–	система управління базами даних
США	–	Сполучені Штати Америки
ТОВ	–	Товариство з обмеженою відповідальністю
ФОП	–	фізична особа – підприємець
ФРН	–	Федеративна Республіка Німеччина
ЦОД	–	Центр обробки даних
ЦОРК	–	Центр оперативного реагування на кіберінциденти
ЦРУ	–	Центральне розвідувальне управління США
ШІ	–	штучний інтелект
ШПЗ	–	шкідливе програмне забезпечення
2FA	–	Two Factor Authentication
AD	–	Active Directory
ADUC	–	Active Directory Users and Computers
AI/ML	–	Artificial Intelligence / Machine Learning
AMP	–	Advanced Mailware Protection
API	–	Application Programming Interface
APT	–	Advanced Persistent Threat
BAS	–	Breach and Attack Simulation
BCP	–	Business Continuity Plan
BYOD	–	Bring Your Own Device
CASB	–	Cloud Access Security Broker
CVE	–	Common Vulnerabilities and Exposures
CCDCOE	–	Cooperative Cyber Defence Centre of Excellence
CCDCOE	–	NATO Cooperative Cyber Defence Centre of Excellence
CEEC	–	Central and Eastern European Countries
CEECI	–	Central and Eastern European countries cybersecurity initiatives
CERT	–	Computer Emergency Response Team
CISO	–	Chief Information Security Officer
CISA	–	Cybersecurity and Infrastructure Security Agency
CoA	–	Change of Authorization
CRM	–	Customer Relationship Management

CSIRT	–	Computer Security Incident Response Team
CVP	–	Closest Vector Problem
CVSS	–	Common Vulnerability Systems
DAST	–	Dynamic Application Security Testing
DDoS	–	Distributed Denial of Service
DLP	–	Data Loss Prevention
DNS	–	Domain Name System
DRP	–	Disaster Recovery Plan
DSA	–	Digital Signature Algorithm
ECC	–	Elliptic Curve Cryptography
EDR	–	Endpoint Detection&Response
EIF	–	Extended Isolated Forest
EMM	–	Enterprise Mobility Management
ENISA	–	European Union Agency for Cybersecurity
EPP	–	Endpoint Protection
ERP	–	Enterprise Resource Planning
ESA	–	ESET Secure Architecture
FIPS	–	Federal Information Processing Standards
FN	–	False Negatives
FTP	–	File Transfer Protocol
FP	–	False Positives
GCI	–	Global Cybersecurity Index
GDPR	–	General Data Protection Regulation
GGE	–	Group of Government Experts
GPS	–	Global Positioning System
HSM	–	Hardware Security Module
HTTP	–	Hypertext Transfer Protocol
IAM	–	Identity and Access Management
IAST	–	Interactive Application Security Testing
IEC	–	International Electrotechnical Commission
IForest	–	Isolated Forest
IIoT	–	Industrial Internet of Things
IoC	–	Indicators of Compromise
IoT	–	Internet of Things
IPS	–	Intrusion Prevention System
ISC	–	Cybersecurity Workforce Study
ISO	–	International Organization for Standardization
ITU	–	International Telecommunication Union
LAN	–	Local Area Network

LDAP	–	Lightweight Directory Access Protocol
M2M	–	Machine-to-Machine
MAC	–	Media Access Control
MAD	–	Microsoft Active Directory
MAM	–	Mobile Application Management
MDM	–	Master Data Management or Mobile Device Management
MDR	–	Managed Detection and Response
MSSP	–	Managed Security Service Provider
MVC	–	Model-View-Controller
NAC	–	Network Access Control
NATO	–	North Atlantic Treaty Organization
NCPI	–	National Cyberpower Index
NCSI	–	National Cyber Security Index
NVD	–	National Vulnerability Database
NFT	–	Non-Fungible Token
NGFW	–	Next-Generation Firewall
NIST	–	National Institute of Standards and Technology
NVR	–	Network Video Recorder
OECD	–	Organisation for Economic Co-operation and Development
OSI	–	Open Systems Interconnection model
OSINT	–	Open Source Intelligence
OSSTMM	–	Open-Source Security Testing Methodology Manual
OTM	–	One-Time Password
OWASP	–	Open Web Application Security Project
PAM	–	Privileged Access Management
PCI DSS	–	Payment Card Industry Data Security Standard
PDoS	–	Permanent Denial of Service
PESCO	–	Permanent Structured Cooperation
PNT	–	Position, Navigation, and Timing
POS	–	Point Of Sale
PUF	–	Physical Unclonable Function
QKD	–	Quantum Key Distribution
RDP	–	Remote Desktop Protocol
RSA	–	Rivest–Shamir–Adleman
SAST	–	Static Application Security Testing
SCADA	–	Supervisory Control And Data Acquisition
SD-WAN	–	Software Defined Wide Area Network

SIEM	–	Security Information and Event Management
SMB	–	Server Message Block
SNMP	–	Simple Network Management Protocol
SOAR	–	Security Orchestration, Automation and Response
SOC	–	Security Operation Center
SOC 2	–	System and Organization Controls
SQL	–	Structured Query Language
SRA	–	Secure Remote Access
SSDLC	–	Secure Software Development Life Cycle
SSDLC	–	Secure Software Development Life Cycle
SSH	–	Secure Shell
SSL	–	Secure Sockets Layer
SVP	–	Shortest Vector Problem
SWG	–	Security Gateways
TCP	–	Transmission Control Protocol
TOR	–	The Onion Router
TRM	–	Trusted Platform Module
UNGGE	–	United Nations Group of Governmental Experts
VLAN	–	Virtual Local Area Network
VM	–	Vulnerability Management
VPN	–	Virtual Private Network
WAF	–	Web Application Firewall
WAN	–	Wide Area Network
WEP	–	Wired Equivalent Privacy
WPA-PSK	–	Wi-Fi Protected Access-Pre-Shared Key
XDR	–	eXtended Detection & Response
ZTNA	–	Zero Trust Network Access

ПЕРЕДМОВА

На сьогоднішній день розроблено ряд глобальних індексів, які дозволяють визначити можливості країни у сфері кіберзахисту, оцінити її кіберпотужність, зокрема спроможність регуляторних заходів та засобів для досягнення стратегічних цілей кібербезпеки. Слід відмітити високий потенціал України в цьому напрямі. Це підтверджується позиціями у світових рейтингах.

Згідно з Національним індексом кібербезпеки (National Cyber Security Index, NCSI), який вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами, Україна на кінець 2021 році піднялася на 24-те місце серед 160 країн та поліпшила свою позицію на 4 пункти порівняно з 2019 роком. За можливостями кіберзахисту національного інформаційного простору Україна наближується до Швейцарії (23-тє місце) та Великобританії (22-ге місце). Водночас згідно з Глобальним індексом кібербезпеки (Global Cybersecurity Index, GCI) Україна посідає 78-ме місце. Порівняно з попереднім роком відбулося зниження на 24 позиції. За Національним індексом кіберпотужності (National Cyberpower Index, NCI),який дозволяє вимірювати ефективність державної стратегії, реагування на правопорушення та боротьби з ними, можливості оборони, розподіл ресурсів, участь приватного сектору, рівень ефективності робочої сили та інновацій у сфері кібербезпеки, у 2020 році Україна посіла лише 26-те місце із 30 країн світу та 10-те місце серед європейських країн. Водночас, слід зауважити, що до рейтингу потрапили ті країни, які мали найбільш розвинуті сили кібербезпеки, що підтверджує наявність в України потенційних можливостей нарощення кіберпотужностей та підвищення рівня інформаційної безпеки.

Потенціал України у сфері кібербезпеки відмічається не лише світовими рейтингами, але й міжнародними організаціями. Зокрема, на початку квітня 2022 року Україну прийнято до складу Об'єднаного центру передових технологій з кібероборони НАТО (Cooperative Cyber Defence Centre of Excellence, CCDCOE) як учасника-контрибутора.

Зазначена позитивна динаміка пов'язана в тому числі з удосконаленням вітчизняного законодавства у сфері інформаційної та кібербезпеки. На сьогоднішній день нормативно-правова база регулювання

та забезпечення безпеки в інформаційному просторі, у тому числі кіберпросторі, включає: Конституцію України, Закон України «Про національну безпеку України», Закон України «Про Концепцію Національної програми інформатизації», Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», Стратегію національної безпеки, Стратегію інформаційної безпеки, Стратегію кібербезпеки України, Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки, Концепцію розвитку цифрових компетентностей, Міжнародні стандарти серії ISO/IEC 27000, нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України стосовно створення і функціонування комплексної системи захисту інформації (КСЗІ), інші нормативно-правові акти, що регулюють відносини у сфері інформаційної безпеки.

Також відмічається посилення співпраці з міжнародними організаціями у сфері кібербезпеки. У вересні 2021 року Державною службою спеціального зв'язку та захисту інформації (ДССЗЗІ) України укладено угоду з Агентством з кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency, CISA), яка передбачає: координацію дій щодо захисту об'єктів критичної інформаційної інфраструктури та вдосконалення системи реагування на кіберінциденти; обмін досвідом у рамках системи управління ризиками (Risk Management), що дозволить забезпечити національну стійкість України до кіберзагроз; використання досвіду США щодо організації взаємодії державних органів та бізнесу у сфері кібербезпеки; реалізацію міжнародних проєктів технічної допомоги щодо побудови мережі галузевих і регіональних операційних центрів безпеки (Security Operation Center, SOC) та команд реагування (Computer Security Incident Response Team, CSIRT), які передбачені Стратегією кібербезпеки України. Приєднання України до складу Об'єднаного центру передових технологій з кібероборони НАТО (Cooperative Cyber Defence Centre of Excellence, CCDCOE), яке відбулося у квітні 2022 року, забезпечує можливість обміну досвідом у виявленні та протидії сучасним кіберзагрозам, відпрацювання навичок спільного реагування на кібератаки та проведення операцій оборони і стримування в кіберпросторі.

Розвиток міжнародної співпраці в напрямку посилення кіберстійкості України є пріоритетним завданням з метою попередження глобальних інформаційних загроз, забезпечення високого рівня якості розслідування кіберзлочинів, затримання і переслідування зловмисних агентів, подолання проблем кібербезпеки.

Водночас існують напрями у сфері кібербезпеки, які негативно впливають на позиції України в зазначених рейтингах та потребують удосконалення. Зокрема, низький рівень внеску на сьогоднішній день у глобальну кібербезпеку, недостатній рівень захисту цифрових послуг, недостатньо розвинений напрям військових кібероперацій.

Слід зазначити, що з початку 2022 року ведеться активна діяльність по всіх зазначених проблемних аспектах: Україна стала активним учасником міжнародного співробітництва у сфері кібербезпеки; йде процес формування кіберструктур, які відповідають за інформаційну і кібербезпеку, захист критичної інфраструктури та кіберрозвідку.

Ураховуючи досягнення України в кіберпросторі, правомірно визначити її рівноправним учасником на міжнародній арені у сфері кібербезпеки. Перспективними завданнями мають стати подальше вдосконалення систем інформаційного та кіберзахисту об'єктів критичної інфраструктури на основі передових технологій і світових практик, а також узгодженість дій із міжнародними організаціями щодо протидії загрозам, пов'язаним із розвитком цифрової економіки та інформаційного суспільства. А побудова ефективної системи національної кібербезпеки для комплексної протидії кіберзагрозам сприятиме формуванню превентивного механізму їх стримування та випереджальному реагуванню на динамічні зміни, що відбуваються в кіберпросторі. Тому монографія присвячена проблемі забезпечення кібербезпеки держави, яка досліджується як у методологічному, так і в організаційно-технічному аспектах. Значну кількість результатів, поданих у монографії, отримано вперше.

Автор висловлює подяку рецензентам: докторам наук, професорам Козловському В.В. та Легоміновій С.В. за цінні зауваження та рекомендації; кандидату наук Старовойтенку О.О. за допомогу в підготовці матеріалів монографії та оформленні до друку.

ВСТУП

Одним зі світових трендів є тенденція до значного зростання кількості кібератак, які стають усе більш витонченими і малопрогнозованими. Особливою метою кіберзлочинців є критично важливі об'єкти інфраструктури країни. У червні 2017 року сталася найбільша кібератака в історії країни, що заблокувала роботу тисяч українських компаній і державних органів. Головною жертвою вірусу-шифрувальника Petya.A стала Україна, де зареєстровано понад 75 % всіх випадків зараження.

Впродовж лише одного дня комп'ютерний вірус Ransom: Win32/ Petya атакував приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади і місцевого самоврядування та ін.

А 12 грудня 2023 року відбулася наймасштабніша в історії глобального телеком-ринку кібератака на мережу «Київстар», що на дві доби повністю зупинила роботу оператора, який забезпечує послугами мобільного зв'язку 50 % абонентів України, зокрема державні установи й силові структури. Збій у роботі найбільшого мобільного оператора країни призвів до непрацездатності частини банкоматів, POS-терміналів (Point Of Sale terminal) та інформативно-платіжних терміналів «ПриватБанку», «Ощадбанку», «Райффайзен Банку», «Правекс Банку», сервісів «Монобанку». Також він негативно вплинув на роботу двох інших українських операторів мобільного зв'язку: у Vodafone збільшився трафік та навантаження на платіжні системи, що спричинило затримки із зарахуванням грошей; у Lifecell відбувалися перебої в роботі застосування своїх абонентів. І лише через вісім днів, 20 грудня, «Київстар» зміг повністю відновити надання всіх послуг як в Україні, так і за кордоном. Ця хакерська атака проти «Київстар» призвела до руйнування близько 40 % його інфраструктури.

2024 рік. Здійснено наймасштабнішу за останній час зовнішню хакерську атаку на державні реєстри України. Було призупинено роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції. Через атаку на державні реєстри в «Дії» тимчасово стали

недоступними 27 послуг, зокрема реєстрація ФОП (фізична особа – підприємець) та ТОВ (Товариство з обмеженою відповідальністю), бронювання працівників від мобілізації, перереєстрація авто, реєстрація права власності на майно, оформлення допомоги дітям, «єОселя», «єВідновлення», подання заяв про шлюб та інші. Сервісні центри Міністерства внутрішніх справ (МВС) також тимчасово призупинили надання окремих реєстраційних послуг, пов'язаних зі зміною власника транспортного засобу.

Держава виявилася не в змозі протистояти таким атакам, які, у свою чергу, виявили незахищеність життєво важливих інтересів людини й громадянина, суспільства і самої держави при використанні кіберпростору та відсутності можливості своєчасного виявлення, попередження й нейтралізації реальних і потенційних загроз національній безпеці в кіберпросторі. Тому проблема забезпечення кібербезпеки держави є надзвичайно актуальною.

РОЗДІЛ 1
ГЛОБАЛЬНІ ВИКЛИКИ І ЗАГРОЗИ В КІБЕРПРОСТОРІ

1.1. Сучасний ландшафт кіберзагроз
1.1.1. Кібератаки: аналітичний вимір

Стрімкий розвиток процесів цифровізації став джерелом не лише нових можливостей, але й ризиків та загроз, у першу чергу інформаційній та кібербезпеці держави. Поряд із традиційними загрозами, такими як втручання сторонніх осіб в інформаційні системи (ІС) і мережі, порушення цілісності баз даних (БД) тощо, створюється ряд додаткових загроз інформаційним ресурсам і технологіям, методи діагностики і протидії яким поки що відпрацьовані не повною мірою. У першу чергу, це загрози, які пов'язані з кібератаками, розкриттям персональних даних, впливом шпигунських програм і вірусів, фішингом, загрозами, пов'язаними з оновленням комп'ютерних програм, тощо. За умов постійного зростання кіберризиків і кіберзагроз важливим є моніторинг рівня кібербезпеки України, висвітлення основних проблем побудови національної системи кібербезпеки та визначення напрямів їх вирішення.

Розвиток ІТ-технологій поряд із безперечними перевагами став причиною поглиблення ризиків та загроз в інформаційному середовищі, зокрема кіберпросторі. Так, якщо на початку 2020 року кількість кібератак у світі становила близько 5 тисяч за тиждень, то на початку 2021 року їхня кількість зросла до 200 тисяч [1]. При цьому 19 % усіх кібератак у світі, зафіксованих у 2021 році, було вчинено проти України (на першому місці серед країн, проти яких спрямовані кібератаки, – Сполучені Штати Америки (США)). Україна посідала друге місце у світових рейтингах за кількістю кібератак, які спрямовані, у першу чергу, на об'єкти критичної інфраструктури країни, тобто такі галузі, як енергетична, фінансова, телекомунікаційна тощо, та державні електронні інформаційні ресурси, порушення функціонування яких є загрозою національним інтересам [2].

З початку 2022 року російська федерація (рф) розгортає кібервійну проти України – інтенсивність кібератак зросла: лише в січні було виявлено вже 6,8 млн підозрілих подій інформаційної безпеки, 25,5 тис. потенційних кіберінцидентів та зупинено 121 кібератаку. Для порівнян-

ня: у квітні 2021 року фахівцями Служби безпеки України (СБУ) було виявлено 1,5 млн підозрілих подій та припинено 53 критичні кіберінциденти [3]. За січень – лютий 2022 року на об'єкти критичної інфраструктури та державні інформаційні ресурси України було здійснено 436 кібератак порівняно з 64 за такий самий період 2021 року [1]. Кібератаки на об'єкти критичної інфраструктури та державні інформаційні ресурси України у січні – лютому 2022 року [1, 2, 4, 5].

За даними ДССЗЗІ, з початку військової агресії рф була зареєстрована критична кількість DDoS-атак за одну добу – 271 [2]. У березні – травні 2022 року кібератаки на енергетичну сферу, логістичну інфраструктуру, сайти українських онлайн-медіа та офіційні державні ресурси продовжувалися.

Основними видами кібератак, які становлять найбільшу загрозу інформаційній безпеці національної економіки, визначено програми-вимагачі, інсайдерські атаки, фішинг, цільові кібератаки та DDoS-атаки (Distributed Denial of Service attack). Їхній деструктивний вплив спричиняє, у першу чергу, значні фінансові втрати. Наймасштабніші кібератаки на об'єкти критичної інфраструктури та державні інформаційні ресурси України:

- кібератака на окремі офіційні вебсайти та системи ІТ-сектору (13.01.2022 р.);
- масштабна кібератака на близько 70 державних вебсайтів, зокрема Міністерства оборони України (МОУ), Міністерства закордонних справ (МЗС), Державної служби з надзвичайних ситуацій (ДСНС), додатка «Дія» та ін., які були побудовані на CMS October компанією Kitsoft (14.01.2022 р.);
- DDoS-атака на державні та банківські сайти України, що тривала понад 5 годин і цілями якої були близько 15 банків, зокрема «ПриватБанк» та «Ощадбанк», а також сайти домену gov.ua (15–16 лютого 2022 р.);
- кібератака вірусом FoxBlade на державні ресурси, ІТ-сферу, енергетику і фінансовий сектор з метою знищення БД (23.02.2022 р.);
- наймасштабніша кібератака на мережу «Київстар», що на дві доби повністю зупинила роботу оператора та призвела до непрацездатності частини банкоматів, POS-терміналів та інформативно-платіжних терміналів «ПриватБанку», «Ощадбанку», «Райффайзен Банку», «Правекс Банку», сервісів «Монобанку» (12.12. 2023 р.).

У 2023 році в Україні кількість кібератак зросла порівняно з 2022 роком на 15,9 % до 2 543 інцидентів. За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA (Computer Emergency

Response Team), 347 кібератак було зафіксовано на уряд та урядові організації, 276 – на місцеві органи влади, 175 – на організації в секторі безпеки та оборони, 127 – комерційні організації (рис. 1.1).

Ще 92 рази атакували енергетичний сектор, 81 – телеком, 38 – освітні установи, 32 – транспортну галузь, 30 – фінансовий сектор, 25 – IT-сектор, 15 – ЗМІ (засоби масової інформації), 12 – медичні установи (рис. 1.2).

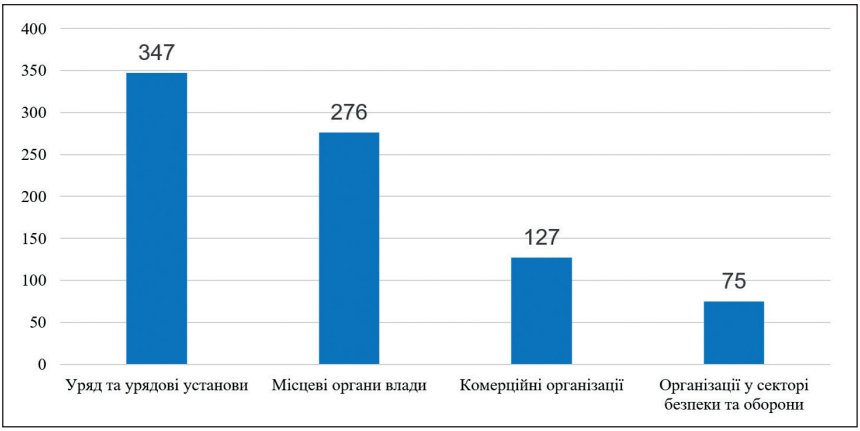

Рис. 1.1. Кібератаки на установи України, 2023 рік

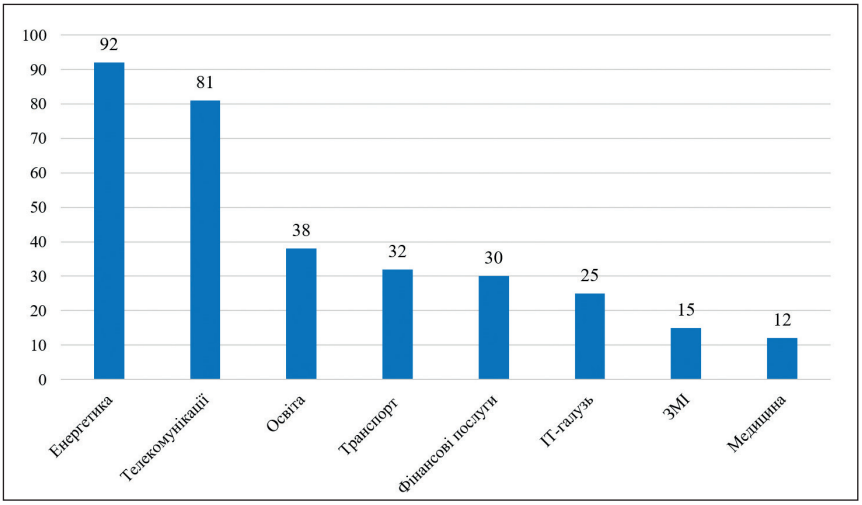

Рис. 1.2. Кібератаки на галузі економіки України, 2023 рік

У ІІІ кварталі 2023 року було зареєстровано 355 кіберінцидентів, що на 46 % вище, ніж у ІІ кварталі поточного року. За цей період найчастіше зустрічалися такі шкідливі програмні забезпечення, як SmokeLoader, Agent Tesla, Formbook, Guloader, StrRAT, RmsRAT і Emotet.

Окрім цього, протягом ІІІ кварталу 2023 року було зафіксовано 202 кібератаки, ініційовані проросійськими хакерськими угрупованнями. До найактивніших проросійських хакерських угруповань, які атакували інформаційні ресурси України, входять «Народная CyberArmy», BLUENET, NoName057(16), PHOENIX і Lira. Кількість кібератак, які були здійснені ними за цей період, становить 9 % від загальної кількості зафіксованих атак, організованих аналогічними угрупованнями. Більшість із них були націлені на фінансовий, урядовий, телекомунікаційний, освітній сектори, а також громадські організації. Лише за другу половину 2023 року зафіксували та розслідували 1,46 тис. кіберінцидентів.

У 2023 році кількість кібератак порівняно з 2022 роком зросла на 15,9 % і становила 2 543 випадки. За підрахунками Держспецзв'язку, загалом за цей рік було виявлено 1 516 861 підозрілих унікальних файлів, при цьому найчастіше виявляли віруси типу SmokeLoader, Agent Tesla, Snake Keylogger, Remcos, Formbook. Крім того, безпосередньо аналітиками безпеки було зафіксовано та опрацьовано 1 105 кіберінцидентів, що на 62,5 % більше, ніж за результатами 2022 року.

У 2024 році кількість кібератак на Україну зросла на 69,8 %, досягнувши 4 315 інцидентів, порівняно з 2023 роком, коли було зафіксовано 2 541 кіберінцидент. Про це повідомляла ДССЗЗІ на своєму сайті.

Найчастіше хакери атакують: місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, телекомунікації. Найпоширеніші типи атак: розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи. Метою хакерів є викрадення чутливої інформації, а також знищення даних та інформаційних систем.

Від початку 2025 року в Україні відбувається близько 15 кібератак щодня. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA фіксує кіберінциденти та відстежує понад 150 кластерів кіберзагроз (UAC). В основному кібератаки здійснюють пов'язані з рф хакери. Ідеться про:

- UAC-0010 або Gamaredon/Primitive Bear/Aqua Blizzard (одна з найбільших загроз у контексті кібератак);

- UAC-0184, UAC-0200 (спеціалізуються на атаках на військовослужбовців);
- UAC-0218 / UAC-0219 (викрадення даних);
- UAC-0050, UAC-0006 (є найактивнішими фінансово вмотивованими кластерами).

Наразі спостерігається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України. Ворог не полишає спроб дестабілізувати нашу країну і за допомогою кіберзброї. Це свідчить про те, що протистояння в кіберпросторі залишається однією з найгарячіших точок війни, а рф продовжить застосовувати всі можливі методи для отримання важливої для неї інформації.

Ураховуючи такі активні дії в кіберпросторі, пріоритетними завданнями для України мають бути: подальше вдосконалення систем інформаційного та кіберзахисту об'єктів критичної інфраструктури на основі передових світових практик, узгодженість дій із міжнародними організаціями щодо протидії загрозам, пов'язаним із розвитком цифрової економіки та інформаційного суспільства, а також побудова ефективної системи національної кібербезпеки для комплексної протидії кіберзагрозам, яка сприятиме формуванню превентивного механізму протидії загрозам та їхньому стримуванню, випереджальному реагуванню на динамічні зміни, що відбуваються в кіберпросторі.

1.1.2. Аналіз сучасних кіберзлочинів

Кібератаки. Це різноманітні загрози, які спрямовані на комп'ютерні системи, мережі та дані з метою завдання шкоди, незаконного доступу, крадіжки інформації або перешкоджання нормальному функціонуванню цифрових систем. Це розширений і різноплановий спектр атак, кожна з яких має свої особливості та наслідки. Далі наведено більш детальний опис різних видів кібератак:

- *Malware* – це загальний термін для шкідливого програмного забезпечення (ПЗ), що охоплює віруси, хробаки, троянці, шпигунські програми та інші види шкідливих програм. Шкідливе ПЗ може впроваджуватися в цільову систему, поширювати інфекцію, збирати чутливі дані або завдавати іншої шкоди;
- *фішинг* – вид атаки, за якої зловмисники видають себе за довірених осіб або організації, щоб обманювати користувачів та примушувати їх подавати особисті чи фінансові дані. Зазвичай це виконується через фішингові листи, які містять підроблені логотипи та логін-форми;

- *атаки з відмовою в обслуговуванні (DDoS)* – полягають у тому, що зловмисники намагаються переповнити сервери або мережі запитами, заблокувавши їх, тим самим призводячи до відмови в обслуговуванні. Це може спричинити недоступність вебсайтів або сервісів;
- *соціальна інженерія* – метод атак, що полягає в обмані людей з метою отримання конфіденційної інформації. Соціальні інженери можуть використовувати соціальні мережі, переконувальні виклади або імітування авторитетних осіб для отримання доступу до систем;
- *атаки на програмні вразливості* – зловмисники можуть використовувати вразливості в програмах або операційних системах (ОС), щоб виконувати зловмисні дії, наприклад уведення шкідливого коду або вимкнення безпеки;
- *атаки на вебдодатки* – зловмисники можуть атакувати вразливі вебдодатки, використовуючи введення даних або інші методи для отримання доступу до БД або викрадення інформації.

Кожен із цих видів кібератак вимагає унікального підходу до кібербезпеки, тому організації мають бути готовими до захисту від широкого спектру загроз у цифровому світі.

Проникнення в дані. Охоплює різноманітні атаки та методи, спрямовані на отримання незаконного доступу до чутливих даних, які зберігаються на комп'ютерах та серверах. Цей вид атаки може призвести до розголошення конфіденційної інформації, викрадення особистих даних або втрати важливої корпоративної інформації. Розглянемо детальніше різні види кібератак, пов'язаних із проникненням у дані:

- *уразливість у ПЗ* – зловмисники використовують відомі або раніше не відомі вразливості в програмах або ОС, щоб отримати доступ до системи;
- *атаки переповнення буфера* – зловмисники намагаються переповнити буфери пам'яті програми введенням даних, які перевищують допустимий обсяг. Це може призвести до виконання шкідливого коду або віддаленого доступу до системи;
- *атаки на засоби аутентифікації* – використовуються для перехоплення паролів або атаки «людина-посередник», щоб отримати доступ до даних, зашифрованих паролем;
- *SQL-ін'єкції* – використовуються для отримання доступу до БД. Зловмисники вставляють SQL-код (Structured Query Language) у вебформи або URL, щоб отримати несанкціонований доступ до даних у базі;
- *атаки на служби та порти* – спрямовуються на відкриті мережеві порти та служби на серверах, шукаючи слабкі місця в їх захисті;

- *файлові атаки* – використовуються шкідливі файли, такі як віруси, хробаки чи троянці, для введення шкідливого коду на комп'ютери або сервери та отримання доступу до системи;
- *атаки на паролі* – включають в себе перебирання паролів, перехоплення паролів під час аутентифікації, а також використання слабких або очевидних паролів для вторгнення;
- *витік даних* – втрата чутливої інформації через різні канали, такі як некоректна конфігурація систем, крадіжка даних або просто недбале поводження з конфіденційною інформацією. Може бути результатом недбалості, внутрішньої загрози або внутрішньої атаки;
- атаки з використанням надмірних прав – отримання доступу до системи з використанням надмірних прав, що дозволяють зловмисникам отримувати доступ до чутливої інформації або змінювати налаштування системи.

Захист від цих видів атак вимагає ретельного моніторингу та оновлення систем, а також надійних методів аутентифікації та авторизації. Також важливо навчати персонал впізнавати потенційні загрози та дотримуватися кращих практик із кібербезпеки.

Атаки вимагання викупу (Ransomware). Це атака, за якої зловмисники шифрують або блокують доступ до даних або системи, після чого вимагають викуп за розшифрування чи відновлення доступу. Розглянемо основні види цих атак:

- *блокувальні Ransomware* – у цих атаках зловмисники блокують доступ до комп'ютера або файлів, роблячи їх недоступними для користувача. Після блокування вони вимагають викуп за відновлення доступу до даних;
- *шифрувальні Ransomware* – цей вид атаки полягає в шифруванні файлів на комп'ютері жертви, після чого зловмисники вимагають викуп за розшифрування. Жертвам надсилаються інструкції щодо оплати вимоги в обмін на ключ для розшифрування файлів;
- *дворівневі Ransomware* – ця атака охоплює обидва методи блокування доступу та шифрування файлів. Зловмисники зазвичай спочатку блокують доступ до комп'ютера та вимагають викуп, а якщо жертва відмовляється платити, файли на комп'ютері шифруються, що ще більше ускладнює відновлення;
- *рейдерські Ransomware* – у цих атаках зловмисники не лише шифрують дані, але й крадуть чутливу інформацію (наприклад, корпоративні документи або персональні файли) перед шифруванням, а потім вимагають викуп не лише за розшифрування, але й за неоприлюднення або продаж викрадених даних;

- *публічний Ransomware* – цей вид атак загрожує розсилати або оприлюднювати чутливі дані жертв, якщо вони не викуплять свою конфіденційність або не квапитимуться оплатити вимогу;
- *порушення безпеки даних із наслідками* – у цих випадках зловмисники можуть видалити або не надати доступ жертві до даних навіть після отримання викупу.

Атаки «Вимагання викупу» можуть бути руйнівними для індивідів та організацій і компаній, тому що вони залишають жертв із важкими виборами щодо сплати вимоги, відновлення даних або втрати важливої інформації. Боротьба із цим типом атак передбачає заходи забезпечення безпеки, резервне копіювання даних, зберігання безпеки та кіберосвіту користувачів, щоб уникнути випадків зараження.

Атаки фішинг і соціальної інженерії. Це методи атак, які спираються на маніпулювання користувачами на психологічному рівні з метою отримання доступу до їхніх даних. Це може бути надсилання фішингових листів або імітація довірчих джерел для обману користувачів. Ось декілька типів цих атак:

- *виманювання логіну і пароля* – надсилання жертві шахрайської електронної пошти, яка маскується під легітимний вебсайт чи сервіс. Ця пошта запитує користувача ввести свій логін та пароль, і якщо користувач це робить, зловмисник має доступ до його облікового запису;
- *спам і фішингові пошти* – надсилання масових спам-повідомлень із фішинговими посиланнями або вкладеннями. Жертви, які відкривають ці пошти або клікають на посилання, можуть стати жертвами фішингу;
- *фішингові вебсайти* – імітують легітимні ресурси, такі як банківські системи, соціальні мережі чи електронні магазини. Жертва може ввести свої дані на такому сайті, і зловмисник отримає їх;
- *телефонний фішинг (вішинг)* – зловмисники телефонують жертвам, представляються працівниками банків, компаній тощо й намагаються отримати конфіденційну інформацію від них;
- *психологічна маніпуляція* – використання психологічних технік для сприяння сценаріям атаки. Наприклад, зловмисник може створити обстановку, де жертва відчуває термінову необхідність надати потрібну йому інформацію;
- *фішинг на основі подій* – використання актуальних подій або глобальних криз (наприклад, пандемії) для створення фішингових кампаній, що привертають увагу і використовують ці події як спосіб маніпуляції жертвами;

- *фішингова атака соціальної мережі* – створюються фіктивні профілі в соціальних мережах для спілкування із жертвами з метою надмірного видавання себе за відому особу чи впливового спеціаліста.

Ці види атак створюють великий ризик для індивідів та організацій і вимагають уважності та навичок для їхнього виявлення та запобігання.

Кібератаки, спонсоровані державами. Це атаки, які здійснюються або підтримуються державними суб'єктами. Вони потребують значних ресурсів та високого рівня координації й можуть мати серйозні наслідки для цілей та інтересів інших держав або приватних суб'єктів. Наведемо короткий опис видів таких кібератак:

- *кібершпигунство* – здійснюється з метою збирання розвідувальної інформації та доступу до важливих даних і систем інших держав;
- *кібервплив на комунікації та ЗМІ* – використання кібертехнологій з метою блокування чи обмеження доступу до Інтернету, соціальних мереж або інших ЗМІ для контролю інформації, яка доходить до їхніх громадян. Може впливати на вибори або політичні процеси, спрямовані на дестабілізацію політичних режимів в інших країнах;
- *кіберпропаганда* – використання кібермедіа для поширення пропаганди, фейків та дезінформації з метою впливу на громадську думку в інших країнах;
- *кібертероризм* – співпраця терористичних угруповань із державами або використання їхніх ресурсів для здійснення кібератак із терористичною метою на критичну інфраструктуру або розповсюдження терористичної пропаганди;
- *кібервійни* – використання кібератак для руйнування інфраструктури інших країн;
- *кіберзлочинність у військовому контексті* – здійснення державних кібератак для реалізації геополітичних інтересів, що може призвести до масштабних міжнародних конфліктів.

Захист від кібератак, спонсорованих державами, вимагає наявності високого рівня кібербезпеки та залучення значних ресурсів для протидії.

1.2. Основні виклики в кіберпросторі

Забезпечення захисту від кібератак – серйозний виклик, який залежить від багатьох факторів, і це є одним із пріоритетних завдань сьогодення. Експерти визначили основні виклики, що існують у кіберпросторі вже зараз та збережуться в найближчому майбутньому [6, 7].

1. Збільшення кількості кібератак. Відповідно до звіту Cybersecurity Ventures, очікується, що глобальні збитки, спричинені кіберзлочинною діяльністю, зростатимуть на 15 % на рік і до 2025 року можуть досягти 10,5 трильйонів доларів щорічно. Причинами такого зростання є значне збільшення активності груп кіберзлочинців та зловмисників, діяльність яких спонсорується державою. Водночас кількість атак зростає внаслідок процесів цифрової трансформації, а також кібервійни, яку веде рф проти України та інших країн.

2. Поява нових витончених тактик кібератак. Одним із різновидів фішингу, який останнім часом активізувався, є гібридний фішинг, що поєднує традиційний метод на основі електронної пошти з вішингом. Цей вид використовується для отримання доступу до систем організації та розгортання шкідливих програм, таких як програми-вимагачі. Під час такої атаки потенційна жертва спочатку отримує електронний лист, наприклад, про продовження підписки на послугу. При цьому в разі бажання скасувати підписку користувач може зателефонувати до служби підтримки за номером телефону, вказаним у повідомленні. Під час дзвінка жертву обманом заманюють встановити шкідливу програму, яка часто може поширюватися на інші пристрої.

Тим часом можливості машинного навчання створювати несправжні голоси швидко розвиваються. Серйозною загрозою є кількість атак, під час яких шахраї використовують інструменти на основі машинного навчання. Зокрема, для імітації голосу директора певної компанії в режимі реального часу, щоб переконати співробітника переказати гроші на рахунок, який насправді належить зловмисникам.

3. Поширення криптовалют. Нові способи використання криптовалюти знаходять не лише користувачі, компанії та державні установи, а й кіберзлочинці. Збільшення кількості схем шахрайства з криптовалютою підтвердило інтерес хакерів до цієї галузі. Не дивно, що виклики, пов’язані з безпекою у світі криптовалют, також часто стають заголовками новин. Використовуючи платформи в галузі криптовалют (Non-Fungible Token, NFT) та ігор, зловмисники часто створюють нові фішингові сайти для викрадення облікових даних користувачів, зокрема,

для входу в криптовалютні гаманці. Тоді як криптовалютні біржі потрапляють під приціл APT-груп (Advanced Persistent Threat). Наприклад, так було викрадено криптовалюту на суму 625 мільйонів доларів США з відеогри Axie Infinity, що пов'язують із кіберзлочинцями Lazarus.

4. Зростання активності в даркнеті. Величезне зростання кримінальної активності в даркнеті за останні роки, особливо після початку пандемії, є серйозною проблемою, яка ще раз показує важливість досліджень у цих мережах Інтернету. Моніторинг даркнету допомагає спеціалістам із кібербезпеки запобігати атакам, розуміти, як думають шахраї та кіберзлочинці, які шкідливі інструменти використовують зловмисники для доступу до систем організацій або для обману користувачів, а також які корпоративні дані поширюються на чорних ринках.

5. Активність програм-вимагачів. Програми-вимагачі все ще залишаються серйозною проблемою, яка потребує від організацій максимального захисту. Зокрема, їм необхідно подбати про інструменти для протидії атакам програм-вимагачів, організацію комплексних навчальних програм із безпеки для співробітників та готовність до відновлення, якщо атака все ж таки трапиться. Починаючи з 2020 року кількість атак програм-вимагачів щорічно зростає вдвічі, залишаючись найбільш руйнівною загрозою для підприємств.

6. Перехід на дистанційну та гібридну роботу. У зв'язку із цифровою трансформацією бізнесів, спричиненою пандемією, багато компаній зіткнулися із проблемами в безпеці корпоративного середовища. Тоді кількість спроб атак на протокол віддаленого робочого столу (Remote Desktop Protocol, RDP) зросла на рекордні 768 % протягом 2020 року, що виявилось одним із найуразливіших місць в інфраструктурі організацій і підприємств. Цей тренд зберігся і навіть посилився з початком повномасштабного вторгнення військ рф в Україну. Тому зараз організаціям і компаніям варто продовжувати належну підготовку та забезпечення можливостей співробітникам, які працюють віддалено, щоб уникнути потенційних ризиків та захиститися від нових атак кіберзлочинців, які постійно шукають нові недоліки кібербезпеки в корпоративних мережах.

7. Дефіцит кваліфікованих спеціалістів із кібербезпеки. В умовах підвищеного попиту на професіоналів у галузі кібербезпеки продовжує зростати дефіцит кваліфікованих кадрів. Згідно з дослідженням ISC2 Cybersecurity Workforce Study, глобальна нестача кадрів у сфері кібербезпеки становить 3,4 мільйона, при цьому 70 % організацій мають незакриті вакансії. Багато держав працюють над зменшенням цього дефіци-

ту, а великі компанії, такі як Google, Microsoft або IBM, запроваджують різні ініціативи, спрямовані на навчання та підвищення кваліфікації людей у сфері кібербезпеки. Так, Всесвітній економічний форум спільно з кількома компаніями запустив освітню онлайн-платформу для окремих осіб та організацій під назвою Cybersecurity Learning Hub. Метою цього проєкту є навчання та вдосконалення навичок спеціалістів із кібербезпеки для забезпечення якісної роботи в цій галузі.

8. Вплив віртуального світу. Прогнози щодо розвитку метавсесвіту показують, що до 2026 року 25 % населення світу проводитиме принаймні 1 годину на день у цьому віртуальному світі. Тому безпека в метавсесвіті є викликом на майбутнє. Ці спільні віртуальні світи для спілкування та ігор безсумнівно призведуть до великої кількості атак та шахрайства. Крім того, технологічні інновації не завжди розробляються з урахуванням правил безпеки та конфіденційності, оскільки пріоритетом є швидший вихід на ринок.

9. Недостатня обізнаність користувачів. Базова проблема, з якою кібербезпека завжди стикатиметься, – це недостатня цифрова обізнаність працівників щодо векторів атак та способів їхнього розпізнання. Тому співробітники є найслабшою ланкою захисту будь-якої організації. Однак завдяки підвищенню обізнаності сучасним загрозам персонал може стати першою лінією кіберзахисту.

Ураховуючи вищеперелічені виклики кібербезпеки, необхідно використовувати сучасні технології, методи та засоби для протидії кіберзагрозам і підвищення рівня кіберзахисту.

Висновки до першого розділу

Стрімкий розвиток процесів цифровізації став джерелом не лише нових можливостей, але й ризиків та загроз у першу чергу інформаційній та кібербезпеці держави. Найчастіше хакери атакують: місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, телекомунікації. Найпоширеніші типи атак: розповсюдження шкідливого програмного забезпечення, фішинг, компрометація облікового запису або системи. Метою хакерів є викрадення чутливої інформації, а також знищення даних та інформаційних систем.

Наразі спостерігається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України. Ворог не полишає спроб дестабілізувати нашу країну і за допомогою кіберзброї. Це свідчить про те, що протистояння в кіберпросторі залишається однією з

найгарячіших точок війни, а рф продовжить застосовувати всі можливі методи для отримання важливої для неї інформації.

Ураховуючи такі активні дії в кіберпросторі, пріоритетними завданнями для України мають бути: подальше вдосконалення систем інформаційного та кіберзахисту об'єктів критичної інфраструктури на основі передових світових практик, узгодженість дій із міжнародними організаціями щодо протидії загрозам, пов'язаним із розвитком цифрової економіки та інформаційного суспільства, а також побудова ефективної системи національної кібербезпеки для комплексної протидії кіберзагрозам, яка сприятиме формуванню превентивного механізму протидії загрозам та їхньому стримуванню, випереджальному реагуванню на динамічні зміни, що відбуваються в кіберпросторі.

Перелік використаних джерел:

1. Microsoft Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. April 27, 2022.

2. Захист інформаційного та кіберпростору. Звіт SIEM. URL: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення: 05.04.2022).

3. Сайт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua (дата звернення: 05.04.2022).

4. Щодо кібератак на сайти державних органів. URL: https://ssu.gov.ua/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv (дата звернення: 05.04.2023).

5. Поліція розпочала кримінальне провадження за фактом кібератак на сайти державних органів. URL: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ (дата звернення: 05.04.2023).

6. 10 викликів кібербезпеки: експерти розповіли, до чого готуватися користувачам та компаніям. URL: https://www.unian.ua/science/10-viklikiv-kiberbezpeki-eksperti-rozpovili-do-chogo-gotuvatisya-koristuvacham-ta-kompaniyam-12033828.html (дата звернення: 05.04.2024).

РОЗДІЛ 2
МЕХАНІЗМ МІЖНАРОДНОЇ КІБЕРБЕЗПЕКИ

В умовах протидії російській гібридній агресії дедалі більше країн робитимуть ставку на мілітаризацію інформаційного простору й розвиток технологій його безпеки. Нинішній рівень інформатизації України в цілому й органів державної влади зокрема засвідчує актуальність загрози використання проти української держави кібернаступальних технологій. Тому Україна надає великого значення своїй міжнародній співпраці в галузі кібербезпеки, активно залучаючись до різних міжнародних колективних зусиль, що сприяють зміцненню кібербезпеки як на національному, так і на міжнародному рівнях [1].

Формування механізму міжнародної кібербезпеки є складним і динамічним процесом, який вимагає співпраці держав, міжнародних організацій, індустрії та експертного співтовариства, оскільки кіберзагрози постійно зростають у масштабі та складності. Ключовими аспектами формування такого механізму є: міжнародні стандарти та норми; міжнародні організації; міжнародна співпраця та двосторонні угоди; сертифікація та валідація продуктів; заходи кібердетеренції; розроблення кіберстратегій [2].

2.1. Міжнародні організації

Існує кілька міжнародних організацій, які відіграють ключову роль у формуванні та сприянні механізму міжнародної кібербезпеки:

1. International Telecommunication Union (ITU)

ITU є спеціалізованою агентурою Організації Об'єднаних Націй (ООН) і зосереджується на технічних аспектах телекомунікацій. Вони ведуть роботу над розробленням стандартів та рекомендацій у сфері кібербезпеки, а також сприяють міжнародній співпраці в цьому питанні.

2. International Organization for Standardization (ISO)

ISO встановлює стандарти для різних галузей, включаючи інформаційну безпеку. Стандарти, такі як ISO/IEC 27001, надають рамки для управління кібербезпекою в організаціях незалежно від їхнього місця знаходження.

3. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)

Група з експертів ООН з питань інформаційної безпеки розробляє звіти та рекомендації щодо поведінки держав у кіберпросторі. Їхні рекомендації сприяють розвитку норм та правил для кібербезпеки.

4. European Union Agency for Cybersecurity (ENISA)

ENISA є агентурою Європейського Союзу, яка сприяє підвищенню рівня кібербезпеки в Європейському Союзі (ЄС). Вони розробляють рекомендації, допомагають у виявленні й вирішенні кіберзагроз та забезпечують координацію на міжнародному рівні.

5. North Atlantic Treaty Organization (NATO)

NATO визнає кіберпростір як один з основних об'єктів для захисту. Альянс розробляє політику та стратегії кібербезпеки, проводить навчання та вправи для своїх членів.

6. Organisation for Economic Co-operation and Development (OECD)

OECD сприяє розвитку рекомендацій та настанов щодо кібербезпеки, зокрема стосовно захисту критичної інфраструктури та обміну інформацією між країнами.

Ці організації взаємодіють та співпрацюють, щоб формувати міжнародні стандарти, рекомендації та стратегії в галузі кібербезпеки й забезпечити безпеку в цьому цифровому середовищі.

2.2. Міжнародні стандарти та норми

Міжнародні стандарти та норми в галузі кібербезпеки є важливим елементом формування механізму міжнародної кібербезпеки. Основні стандарти та норми, які визначають цю галузь:

1. ISO/IEC 27001 та ISO/IEC 27002

ISO/IEC 27001 встановлює вимоги до системи управління інформаційною безпекою, а ISO/IEC 27002 надає конкретні рекомендації та практики з імплементації цих вимог. Обидва стандарти визначають основні принципи кібербезпеки, такі як захист інформації та управління ризиками.

2. Норми ITU-T X.509

Ці норми визначають формати сертифікатів для захисту ключів та інших даних у системах криптографічного захисту. Вони відіграють ключову роль у впровадженні публічного ключа та обміні інформацією безпеки.

3. IEEE 802.1X

Стандарт IEEE 802.1X визначає механізми аутентифікації в бездротових мережах та інших елементах мережевої інфраструктури. Цей стандарт сприяє захисту від несанкціонованого доступу до мережевих ресурсів.

4. NIST Cybersecurity Framework

Рамковий документ Національного інституту стандартів та технологій США (National Institute of Standards and Technology, NIST) визначає базові принципи кібербезпеки та надає рекомендації щодо захисту критичних інфраструктур. Він визначає кібербезпечні функції, такі як захист, виявлення, відповідь та відновлення.

5. Поведінка держав в Інтернеті

Група урядових експертів (Group of Government Experts, GGE) ООН з питань інформаційної безпеки визначає норми та правила поведінки держав у кіберпросторі. Їхні звіти визначають, як держави поводитися в мережі, у тому числі під час кіберконфліктів.

6. EU General Data Protection Regulation (GDPR)

GDPR встановлює стандарти для захисту особистих даних громадян ЄС. Він регулює обробку та передання цих даних, визначаючи високі стандарти кібербезпеки для компаній, які працюють з особистими даними.

7. Гармонізовані норми ЄС для кіберзахисту критичних інфраструктур

Європейська комісія розробляє гармонізовані норми для забезпечення кіберзахисту критичних інфраструктур, які визначають вимоги та заходи для захисту ключових секторів від кіберзагроз.

Ці стандарти та норми також визначають рамки та керуючі принципи для розвитку та впровадження стратегій кібербезпеки як на національному, так і на міжнародному рівнях.

2.3. Міжнародна співпраця та двосторонні угоди

Двосторонні угоди та міжнародна співпраця в галузі кібербезпеки відіграють важливу роль у забезпеченні безпеки в цифровому середовищі [3]. До них відносяться:

1. Інформаційний обмін

Держави можуть укладати угоди про обмін інформацією щодо кіберзагроз, виявлення нових загроз та методів атак. Це може бути обмін інформацією про сигнатури загроз, аномалії у виявленні та реагуванні на інциденти.

2. Забезпечення правопорядку

Країни можуть укладати угоди про екстрадицію та правову допомогу у справах кіберзлочинності. Це допомагає у притягненні до відповідальності осіб, які вчиняють кіберзлочини, та сприяє покаранню винних.

3. Спільні навчальні програми

Країни можуть розвивати спільні навчальні та тренувальні програми для підготовки кадрів у сфері кібербезпеки. Це дозволяє підвищувати кваліфікацію фахівців та забезпечувати високий рівень експертизи в галузі кіберзахисту.

4. Експертні робочі групи

Держави можуть створювати спільні експертні групи для вивчення та аналізу конкретних кіберзагроз. Ці групи можуть визначати кращі практики, обмінюватися дослідженнями та спільно розробляти стратегії відповіді.

5. Міжнародні конференції та участь у форумах

Країни можуть активно брати участь у міжнародних конференціях та форумах із кібербезпеки. Такі заходи дозволяють обмінюватися поглядами на глобальні проблеми та вирішувати їх спільно.

6. Забезпечення стабільності кіберпростору

Двосторонні угоди можуть передбачати зобов'язання щодо запобігання атакам на критичну інфраструктуру та забезпечення стабільності кіберпростору.

7. Спільні ініціативи з розроблення технічних стандартів

Країни можуть спільно працювати над створенням та розробленням технічних стандартів у галузі кібербезпеки, щоб забезпечити взаємну сумісність та ефективність заходів із захисту.

Двостороння та багатостороння співпраця відіграє ключову роль у забезпеченні стабільності та безпеки кіберпростору на міжнародному рівні.

2.4. Сертифікація та валідація продуктів у сфері кібербезпеки

Сертифікація та валідація продуктів у сфері кібербезпеки відіграють ключову роль у забезпеченні високого рівня безпеки та взаємній сумісності в міжнародному кіберпросторі. Міжнародні організації, такі як Міжнародна організація зі стандартизації (International Organization for Standardization, ISO) та Інтернаціональна електротехнічна комісія (International Electrotechnical Commission, IEC), розробляють стандарти для кібербезпеки. Продукти, що відповідають цим стандартам, можуть отримати сертифікати відповідності.

Common Criteria (ISO/IEC 15408) є міжнародним стандартом для оцінки безпеки IT-продуктів. Виробники можуть пройти процес сертифікації, щоб довести, що їхні продукти відповідають визначеним безпечним стандартам.

Федеральні стандарти обробки інформації у США (Federal Information Processing Standards, FIPS) визначають критерії безпеки для федеральних систем інформаційної обробки. Продукти, які відповідають FIPS, можуть бути використані в урядових системах.

Продукти в різних сферах, таких як мережеві пристрої, антивіруси, криптографічне ПЗ, можуть проходити сертифікацію для визначених стандартів. Наприклад, криптографічні алгоритми можуть бути сертифіковані Національним інститутом стандартів та технологій (NIST) у США.

Деякі специфічні галузі, такі як медицина, фінанси чи енергетика, можуть мати власні вимоги щодо кібербезпеки. Продукти, що використовуються в цих галузях, повинні проходити валідацію відповідно до специфічних вимог.

Важливу роль відіграє міжнародний обмін сертифікованими продуктами, коли продукт отримує сертифікат відповідності міжнародним стандартам. Це полегшує його використання в різних країнах та організаціях, сприяючи гармонізації підходів до кібербезпеки.

Отже, сертифікація та валідація відіграють ключову роль у розвитку та забезпеченні високих стандартів кібербезпеки на міжнародному рівні.

2.5. Заходи кібердетеренції

Це комплекс заходів та стратегій, спрямованих на виявлення, відстеження та відповідь на кібератаки. Ці заходи важливі для формування механізму міжнародної кібербезпеки. До них належать такі:

- виявлення інцидентів – це такі механізми, як системи моніторингу безпеки та інтелектуальні системи аналізу, що допомагають виявляти аномалії та потенційні загрози в реальному часі;
- кіберрозвідка – збирання інформації про кіберзагрози, їхні характеристики та методи використання, що дозволяє визначити можливі джерела атак та розробляти стратегії протидії;
- атака змішаних тактик – розроблення та використання заходів кібердетеренції, що поєднують технічні, правові та організаційні аспекти, спрямовані на підвищення стійкості та варіативності оборони;

- міжнародний обмін інформацією – створення механізмів для міжнародного обміну інформацією про кіберзагрози та інциденти, що дозволяє ефективніше реагувати та спільно боротися з кіберзлочинністю;
- симуляції та тренування – проведення симуляцій кібератак та тренувань для кіберзахисників, що сприяє розвитку навичок та вдосконаленню стратегій оборони;
- співпраця та координація – встановлення міжнародних механізмів співпраці між кіберзахисними агентствами, правоохоронними органами та приватним сектором для обміну інформацією та координації дій;
- юридичні заходи – розроблення міжнародних юридичних норм та угод, які визначають правила та відповідальність у кіберпросторі;
- кібердипломатія – для вирішення кіберконфліктів та встановлення міжнародних стандартів у кібербезпеці.

Усі ці заходи утворюють комплексний механізм, спрямований на підвищення стійкості, виявлення та відповідь на кіберзагрози на міжнародному рівні.

2.6. Розроблення кіберстратегій

Розроблення кіберстратегій є ключовою складовою формування механізму міжнародної кібербезпеки. Вона містить:

- визначення загальних принципів (країни можуть розробляти свої кіберстратегії, визначаючи загальні принципи та цілі, спрямовані на підвищення кібербезпеки, наприклад, забезпечення недопущення кібератак на критичну інфраструктуру);
- створення інституційних механізмів (країни можуть встановлювати інституції та агентства, які відповідають за реалізацію та виконання стратегій, наприклад, створення національних центрів кіберзахисту);
- міжнародна співпраця (кіберстратегії часто передбачають міжнародну співпрацю, наприклад, взаємодія з іншими країнами для обміну інформацією про кіберзагрози та спільного реагування на інциденти);
- норми та правила поведінки (розроблення кіберстратегій може сприяти формулюванню міжнародних норм та правил поведінки в кіберпросторі, наприклад, визначення правил відповідальності за кібератаки);
- захист критичної інфраструктури (країни можуть включати стратегії забезпечення захисту критичної інфраструктури від кіберзагроз для таких секторів, як енергетика, транспорт, телекомунікації та інші);

- боротьба з кіберзлочинністю (кіберстратегії можуть передбачати заходи для боротьби з кіберзлочинністю та кібершахрайством як на національному, так і на міжнародному рівні);
- розроблення технічних засобів (країни можуть включати у свої кіберстратегії розроблення технічних рішень та інновацій для захисту від кіберзагроз);
- участь у міжнародних організаціях (країни можуть приєднуватися до міжнародних організацій, таких як Інтерпол чи ООН, для спільних зусиль у сфері міжнародної кібербезпеки).

Отже, розроблення та реалізація кіберстратегій дозволяють країнам ефективно управляти та реагувати на загрози в кіберпросторі, сприяючи формуванню загальносвітового механізму міжнародної кібербезпеки.

2.7. Формування механізму міжнародної кібербезпеки

Конвенція Ради Європи про кіберзлочинність (Будапештська Конвенція) (2001 р.) є найбільш вагомим і визнаним міжнародно-правовим документом у сфері боротьби з міжнародною та національною кіберзлочинністю [4]. Україна не лише підписала, але й ратифікувала його 10 березня 2006 року. Київ долучився до реалізації проєкту Ради Європи та ЄС «Кіберзлочинність@Східне партнерство» [5] в 2011 році, мета якого полягає в імплементації Будапештської конвенції, удосконалення національного законодавства у сфері боротьби з кіберзлочинністю та налагодження державно-приватного партнерства в цій сфері.

У вересні 2014 року Верховна Рада України (ВРУ) ратифікувала Угоду про Асоціацію між Україною та ЄС, Європейським Співтовариством з атомної енергії та їхніми державами-членами [6]. Одна з вимог згаданої Угоди – наблизити українське законодавство до права ЄС. У ст. 3 додатка XVII зазначено, що згідно зі ст. 114, 124, 133 та 139 гл. 6 «Підприємницька діяльність, торгівля послугами та електронна торгівля» Україна на постійній основі впроваджуватиме чинне законодавство ЄС у свою національну систему. У всіх відповідних документах ЄС вказується, що реформа правового регулювання захисту персональних даних має пряме відношення до врегулювання питань кіберзахисту й забезпечення мережевої та інформаційної безпеки. Стало відомо, що апарат Уповноваженого ВРУ з прав людини готує неофіційні переклади документів щодо питання кібербезпеки в Україні і планує створювати Робочу групу з наближення українського законодавства до європейських стандартів у

сфері захисту персональних даних [7]. Важливість питання захисту персональних даних суттєво зросла після початку дії безвізового режиму. Слід зауважити, що існують такі елементарні заходи безпеки, які можуть забезпечити захист:

- впровадження процесу управління персонального оновлення на всіх вузлах інфраструктури організації;
- впровадження сегментації мережі (поділу мережі на різні сегменти);
- створення, підтримка та тестування плану реагування на інциденти кібербезпеки;
- впровадження процесу резервного копіювання даних (особливо на віддалений носій).

Серед додаткових заходів безпеки: здійснення моніторингу мережевих подій, впровадження обладнання з функцією запобігання вторгненням у комп'ютерних мережах (Intrusion Prevention System, IPS) [8].

В Європі для всіх країн-членів ЄС була прийнята директива про загальні заходи безпеки мережевих та інформаційних систем у ЄС 2016/1148 [9]. Директива зобов'язує держави-члени визначити об'єкт критичної інфраструктури в різних сферах.

У жовтні 2017 року ВРУ ухвалила закон «Про основні засади забезпечення кібербезпеки України», який набрав чинності 9 травня 2017 року [10]. У документі визначено основи забезпечення захисту національних інтересів України в кібернетичному просторі, повноваження державних органів влади, принципи координації їхньої діяльності задля кібернетичної безпеки. Закон також передбачає поглиблення міжнародної співпраці у сфері захисту кіберпростору передусім з ЄС і НАТО.

У США підтримали діяльність українських законотворців, і в лютому 2018-го конгресмени схвалили проєкт Закону про співпрацю з Україною з питань кібербезпеки, спрямований на просування активної взаємодії між Україною та США у сфері кібербезпеки [11]. Законопроєкт розроблено під керівництвом члена комітету з міжнародних справ палати представників Брендана Бойла – безпосередньо для української держави.

Експерти зазначають, що це перший закон США у сфері кібербезпеки, де слово «Україна» винесено в заголовок. При цьому в тексті згадується Будапештський меморандум, і Україні пропонується разом із США виконувати лідерську роль у поліпшенні кібербезпеки у всій Центральній та Східній Європі. Закон свідчить про відповідальне ставлення наддержави до безпеки в регіоні. Підтверджується прихильність США

Хартії про стратегічне партнерство між США і Україною та прихильність США до підтримки співпраці між НАТО та Україною [12].

У Законі США про співпрацю з Україною з питань кібербезпеки містяться певні положення, які фактично є зобов'язаннями для американської влади. Наприклад, Державному Секретарю – вживати заходів, відповідно до інтересів США, щодо допомоги Україні в підвищенні її кібербезпеки. Департамент енергетики буде нести відповідальність для створення українсько-американської робочої групи з розроблення Програми кібернетичної безпеки України. Тобто є чіткі положення, що це – завдання Держдепу та Міністерства енергетики, і чим саме вони мають допомогти українській стороні [13]. Встановлюється формат відносин, констатується, якими вони повинні бути, оскільки до цього часу офіційних документів, у яких це закріплено, не існувало. Американська влада має робити певні кроки щодо захисту критичної інфраструктури.

Проте варто зазначити, що поняття «кібербезпека» в документі стоїть далеко не на першому місці. Велика частина його положень підтверджує інші двосторонні американсько-українські ініціативи: США повинні допомогти Україні в боротьбі з російською пропагандою в соціальних мережах, а також розширити співпрацю по лінії політики, економіки, торгівлі і культури. Зокрема, США мають організувати допомогу щодо захисту урядових українських комп'ютерних мереж, обмін інформацією, позбавлення від російського програмного забезпечення. Це рамковий документ, який дозволяє почати ефективний двосторонній діалог. А як він буде наповнюватися – залежить від учасників діалогу, від комісії, яка буде працювати як у США, так і в Україні.

Восени 2017 року в Гельсінкі в районі Серняйнен офіційно розпочав роботу Європейський центр із протидії гібридним загрозам на чолі з начальником відділу Поліції безпеки Фінляндії (Supo) Матті Саарелайненом. Відомо, що до проєкту долучилися США та європейські держави, включаючи Великобританію, Іспанію, Німеччину, Францію, Норвегію, Швецію, Польщу, і колишні радянські республіки Прибалтики. Основне фінансування структури здійснюється за рахунок Фінляндії. Як заявив на семінарі в день відкриття Центру заступник Генерального секретаря НАТО Арндт Фрейтаг фон Лорінгхофен, «Росія є однією з країн, за якою ведеться спостереження в Центрі».

У вересні 2017 року на саміті із цифрових технологій президент Литви Даля Грібаускайте виступила з ініціативою «кібернетичного Шенгену» – створення в рамках ЄС сил швидкого реагування на кібернетичні атаки. На її думку, дана структура буде доповнювати НАТО в боротьбі

з гібридними загрозами, тероризмом і допомоги третім країнам. Уже в грудні учасники європейської програми Постійного структурованого співробітництва (Permanent Structured Cooperation, PESCO) схвалили надання взаємодопомоги для забезпечення кібернетичної безпеки і створення кібергрупи швидкого реагування, включивши цю ініціативу в число 17 затверджених проєктів. Як зазначають європейці, створення таких сил виведе взаємодію держав ЄС в кібернетичній сфері на новий рівень, коли країни-учасниці не обмежуватимуться лише національним форматом. Керуватиме проєктом Литва.

Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021, МЗС України здійснює координацію взаємодії з міжнародними партнерами в контексті забезпечення кібербезпеки країни [2]. Така міжнародна співпраця України спрямована на розвиток її партнерських відносин та участі у виробленні спільних заходів з реагування на кібератаки і подолання кризових ситуацій у кібербезпеці. У рамках такої співпраці відбувається обмін інформацією, цінним досвідом та найкращими практиками, проведення спільних кібероперацій та розслідувань міжнародних кіберзлочинів, регулярні кібернавчання та тренінги тощо.

На виконання Стратегії кібербезпеки України МЗС країни протягом останніх років уперше провело низку двосторонніх міжвідомчих консультацій із державами-партнерами з посилення взаємодії в галузі кібербезпеки та покращення досвіду реагування на сучасні виклики і загрози в кіберпросторі, зокрема з такими державами-партнерами, як Японія, Сінгапур, Малайзія, Фінляндія, США, Федеративна Республіка Німеччина (ФРН), Велика Британія, Естонія, Нідерланди. 29 вересня 2022 року відбувся другий раунд Діалогу Україна – ЄС з питань кібербезпеки.

З метою посилення стійкості національної критичної інфраструктури з кібербезпеки Україна широко залучена до міжнародної співпраці з реагування на кіберінциденти, маючи доступ до передового світового досвіду та сучасних алгоритмів протидії. Розвиток міжнародної взаємодії у сфері забезпечення кібербезпеки та регулярна участь у міжнародних заходах зі зміцнення довіри в кіберпросторі посилюють спроможності України в цій сфері. Як держава-засновниця ООН й учасниця Організації з безпеки і співробітництва в Європі (ОБСЄ) Україна робить свій внесок у діяльність низки робочих органів цих організацій із кібербезпеки. Україна щільно співпрацює з Європейською агенцією з кібербезпеки (European Union Agency for Cybersecurity, ENISA), входить до

складу Ініціативи з кібербезпеки країн Центральної та Східної Європи (Central and Eastern European countries cybersecurity initiatives, CEECI) та Міжнародного союзу зв'язку (International Telecommunication Union, ITU). 16 травня 2023 року в Таллінні, у штаб-квартирі Об'єднаного центру передових технологій з кібероборони НАТО (Cooperative Cyber Defence Centre of Excellence, CCDCOE), піднято прапор України на знак офіційного приєднання України до цієї установи.

Отже, Україна бере активну участь у діяльності багатьох авторитетних міжнародних організацій, об'єднань та ініціатив, які опікуються спільним виробленням норм поведінки в кіберпросторі та вдосконаленням відповідної міжнародної нормативно-правової бази.

Висновки до другого розділу

Формування системи забезпечення міжнародної кібербезпеки визначається ступенем політичної довіри між урядами держав з урахуванням принципів взаєморозуміння, рівноправності й узгодженості інтересів. Очевидною є необхідність ведення діалогу з усього спектру цих питань, розроблення та вдосконалення міжнародних договорів і національного законодавства у сфері кібербезпеки. Неодмінною умовою вирішення питань щодо правового та організаційного забезпечення кібербезпеки є розуміння того, що держава знаходиться в нерозривному зв'язку та взаємодії з іншими аналогічними структурами і суб'єктами, реалізуючи функції стратегічного і тактичного партнерства, співпраці й добросусідства.

Питання кібербезпеки здатні ускладнити міжнародні відносини, призвести до кібервійни, тому вкрай необхідним є посилення взаємодії між країнами світу щодо неприпустимості зростання напруженості у світовому кіберпросторі.

Отже, забезпечення міжнародної безпеки у світовому кіберпросторі вимагає не лише зусиль окремих країн світу, а й розроблення та вжиття максимально ефективних міжнародних інструментів. Тому всі економічні та політичні ресурси з протидії загрозам міжнародної інформаційної та кібербезпеки повинні розглядатися на найвищому світовому рівні за участю основних кібердержав. Забезпечення кібербезпеки в контексті глобальних загроз, поряд зі спільними зусиллями міжнародного співтовариства, диктує важливість розроблення та вжиття превентивних дієвих заходів проти кібератак і кіберзлочинів у світовому кіберпросторі.

Перелік використаних джерел:

1. Анатолій Худолій. Кібербезпека: сучасні виклики перед Україною. *Acta De Historia & Politica: Saeculum XXI*. № 1. 2019. С. 138–146.

2. Лисецький Ю. М., Старовойтенко О. О., Семенюк Ю. В. Формування механізму міжнародної кібербезпеки // *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Державне управління.* 2024. Т. 35 (74) № 1. С. 184–189.

3. Войціховський А. В. Кібербезпека як напрям євроатлантичної інтеграції України // Право і безпека у контексті європейської та євроатлантичної інтеграції: зб. статей та тез наукових повідомлень за матеріалами дискусійної панелі II Харківського міжнародного юридичного форуму, м. Харків, 28 вересня 2018 р. / редкол.: Ю. Г. Барабаш, Т. М. Анакіна, Д. В. Аббакумова. Харків : Право, 2018. С. 42–48.

4. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки // Міжнародні відносини. 2018. № 18-19 (2). URL: https://cutt.ly/GQCBYfV (дата звернення: 16.12.2024).

5. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 16.12.2024).

6. Угода про асоціацію між Україною, з однієї сторони, та ЄС, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 16.12.2024).

7. Кольцов М., Приходько О. & Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Київ : ГО «Лабораторія законодавчих ініціатив». URL: https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka-1-1.pdf (дата звернення: 16.12.2024).

8. Intrusion Prevention System. URL: https://docs.netskope.com/en/intrusion-prevention-system/ (дата звернення: 16.12.2024).

9. ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text (дата звернення: 16.12.2024).

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. // ВРУ. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.12.2024).

11. У США прийняли законопроект про підтримку кібербезпеки України. URL: https://fakty.com.ua/ua/svit/20180208-u-ssha-pryjnyaly-zakonoproekt-pro-pidtrymku-kiberbezpeky-ukrayiny/ (дата звернення: 16.12.2024).

12. Хартія Україна – США про стратегічне партнерство. URL: https://ua.usembassy.gov/uk/our-relationship-uk/u-s-ukraine-charter-strategic-partnership-uk/ (дата звернення: 16.12.2024).

13. Кібербезпека України: американці зробили перший крок. URL: https://www.ukrinform.ua/rubric-polytics/2399996-kiberbezpeka-ukraini-amerikanci-zrobili-persij-krok.html (дата звернення: 16.12.2024).

РОЗДІЛ 3
КОНЦЕПТУАЛЬНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

3.1. Концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки

У сучасних мінливих умовах усе частіше виникають проблеми соціально-економічної, технологічної і правової взаємодії суб'єктів інформаційно-комунікаційних технологій із виділенням особливої ролі інформаційного суспільства, стратегія розвитку якого в Україні підкреслюється особливою значущістю державного регулювання для впровадження заходів щодо формування національної безпеки країни. Інформаційно-комунікаційні технології активно впливають на розвиток суспільства і держави, тому проблема пошуку дієвих механізмів державного регулювання у сфері інформаційно-комунікаційних технологій є досить актуальною [1].

У системі формування та зміцнення національної безпеки України, безумовно, визначальну роль відіграє ефективне державне регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки та кібербезпеки, але концептуальні засади державного регулювання сфери інформаційно-комунікаційних технологій та їхній вплив на формування і зміцнення національної безпеки залишаються ще не достатньо дослідженими [2].

Одне з основних завдань сучасного курсу соціально-економічних перетворень в Україні, а також формування механізмів зростання національної безпеки полягає в модернізації регулівних функцій держави у сфері застосування всіма суб'єктами в процесі свого функціонування та життєдіяльності інформаційно-комунікаційних технологій. Розвиток та постійне поширення сфер використання інформаційно-комунікаційних технологій є глобальною тенденцією науково-технічного прогресу останніх десятиліть, що приводить до значущих змін у багатьох сферах людської діяльності [3]. Перехід до інформаційного суспільства зумовило якісні перетворення механізмів державного управління у сфері інфор-

маційно-комунікаційних технологій [4]. Основна мета цих реформ полягає в підвищенні ефективності та безпечності державного управління на базі використання нових інформаційно-комунікаційних технологій, без яких сучасний ступінь соціально-економічної ефективності розвинених держав не може бути досягнутий. У нашому дослідженні на основі узагальнення наукових джерел [4, 5] пропонуються такі основні напрямки проведення перетворень (рис. 3.1).

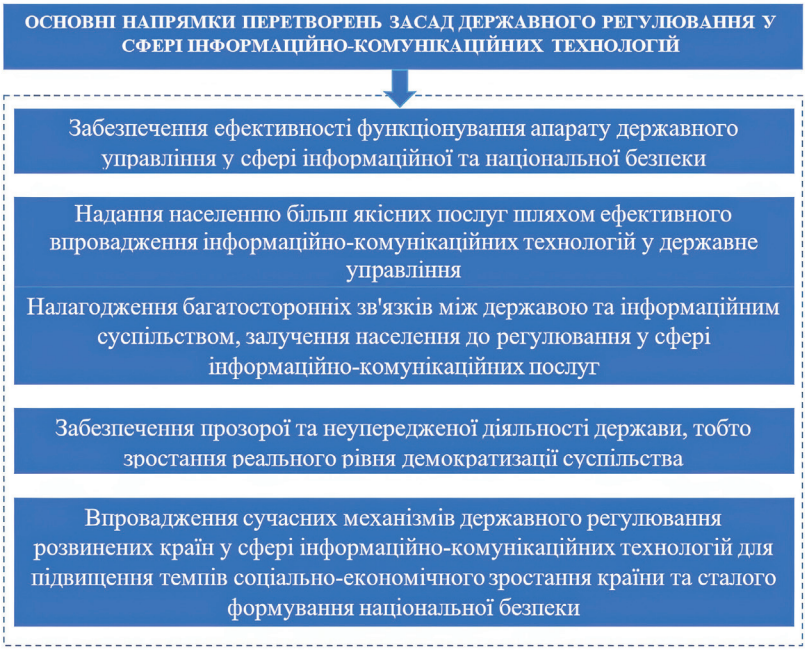

Рис. 3.1. Основні напрямки перетворень засад державного регулювання у сфері інформаційно-комунікаційних технологій

Виходячи з рис. 3.1 та сучасних соціально-економічних, техніко-технологічних та загальнонаукових реалій України, можна виділити проблеми реалізації запропонованих напрямків перетворень засад державного регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки та кібербезпеки, зокрема:

- невиправдано високі витрати та тривалий термін виконання, що призводить до неможливості отримання позитивного ефекту в короткостроковому періоді, а також до ситуації, коли ці заходи перестануть фінансуватися та впроваджуватися в довгостроковому періоді;

- низька ефективність використання бюджетних коштів у результаті відсутності кваліфікованого керівництва з боку державних управлінців та корупційної складової, що може призвести до загроз і небезпек інформаційній, кібер- та національній безпеці країни;
- високий ступінь проєктних ризиків та відсутність розуміння в громадськості щодо заходів державного регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки і кібербезпеки;
- низький ступінь масштабованості та інтеграції систем державного регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки і кібербезпеки з нагальними потребами соціально-економічного розвитку та формування механізмів зміцнення національної безпеки країни;
- низький рівень розвитку державно-приватного партнерства у сфері інформаційного захисту та кіберзахисту.

Треба зазначити, що успішне подолання вищенаведених проблем можливе лише за рахунок ефективного й сталого функціонування системи органів державної влади, що здійснюють державне регулювання у сфері інформаційно-комунікаційних технологій, інформаційної безпеки та кібербезпеки. При цьому регулювання в загальних рисах має здійснюватися Президентом України, ВРУ, Урядом України, Національним банком України (НБУ), а також судами всіх рівнів, до повноважень яких можна віднести, зокрема: розроблення та прийняття стратегії впровадження в державну діяльність інформаційно-комунікаційних технологій та захист їх від неправомірного використання; удосконалення державних програм розвитку та захисту в інформаційно-комунікаційний сфері; реалізацію інформаційних прав фізичних і юридичних осіб; державний контроль і нагляд в інформаційній сфері як ключовий фактор формування та зміцнення національної безпеки країни.

Зазначимо, що інформаційна безпека та кібербезпека країни, регіону та/або муніципального утворення, будучи ключовим фактором формування й зміцнення національної безпеки, є одним з істотних напрямів державного регулювання в інформаційно-комунікаційний сфері, що забезпечує сталий соціально-економічний розвиток відповідних територій.

Під «інформаційною безпекою» у нашому дослідженні будемо розуміти стан захищеності життєво важливих інтересів особистості, інформаційного суспільства та держави від зовнішніх і внутрішніх загроз й небезпек в умовах широкого використання інформаційно-комунікацій-

них технологій у всіх сферах їхньої життєдіяльності. При цьому реалізація заходів інформаційної безпеки дозволяє належним чином забезпечити права суб'єктів на достовірну інформацію, одержувану законним способом, захищати різного роду конфіденційну інформацію, зберігати і примножувати культурні та духовно-моральні цінності, історичні традиції й норми суспільного життя країни.

Під «кібербезпекою» розумітимемо забезпечення захисту цифрових даних, інформаційних систем та інформаційно-технологічної інфраструктури від загроз і атак, з використанням інформаційно-телекомунікаційних систем.

Слід також зазначити, що система інформаційної безпеки і кібербезпеки в державному секторі сформована для інформації, яка є власністю держави, а не всієї існуючої інформації громадян і бізнесу.

Виходячи з вищесказаного, можна сформулювати основні напрямки державного регулювання щодо реалізації заходів інформаційної і кібербезпеки країни, регіону та/або муніципального утворення (рис. 3.2).

Рис. 3.2. Напрями державного регулювання щодо реалізації заходів інформаційної, кібер- та національної безпеки

Як видно, усі п'ять напрямів взаємопов'язані між собою й спрямовані не лише забезпечення інформаційної і кібербезпеки, а й на формування та зміцнення національної безпеки країни. Отже, набуває нагальної необхідності розроблення механізмів щодо координації дій у сфері забезпечення інформаційної і кібербезпеки у зв'язку зі складністю наявних проблем і взаємопов'язаності напрямків діяльності. Забезпечити таку координацію лише органами влади на рівні держави практично неможливо, тому доцільно, щоб система, яка координує дії у сфері інформаційно-комунікаційної безпеки, була розподілена за трьома рівнями (державним, регіональним та місцевим), а також відображала структуру науково-технічних та соціально-економічних проблем. При цьому основними координованими проблемами на регіональному та місцевому рівнях утворень будуть такі:

1. Розроблення моделей загроз інформаційній і кібербезпеці та прогноз реалізації їхніх наслідків для регіону або місцевого утворення.

2. Забезпечення ефективної законодавчої бази щодо захисту інформаційного ресурсу суб'єктів державного регулювання у сфері інформаційно-комунікаційних технологій, включаючи інформацію обмеженого доступу.

3. Систематизація, облік і забезпечення доступу до державного і недержавного інформаційних ресурсів суб'єктів державного регулювання на основі єдиних правових норм.

4. Забезпечення загальнодоступності інформаційно-комунікаційних мереж типу Інтернет та здійснення контролю за його користуванням відповідно до чинного законодавства для запобігання загрозам інформаційної, кібер- та національної безпеки.

5. Виявлення і припинення поширення тенденційних і неправдивих відомостей, маніпулювання суспільною та особистою свідомістю населення й органів влади.

6. Запобігання злому інформаційних систем і копіювання інформації шляхом створення інформаційних систем захисту в регіоні або місцевому утворенні.

7. Запобігання загрозам тероризму по відношенню до об'єктів інформаційно-комунікаційної інфраструктури територій.

8. Забезпечення державних і місцевих структур висококваліфікованими фахівцями з інформаційної, кібер- та національної безпеки.

Для реалізації загальної координації щодо вирішення вищенаведених проблем має ефективно функціонувати відповідна повноважна державна структура з проблем інформаційної і кібербезпеки, яка визна-

чала б специфічні підходи і методи їхнього розв'язання та подолання. Водночас пропонується впровадити мережу координаційних рад, яка буде функціонувати при найбільш компетентних державних і приватних підприємствах, установах та організаціях. Основним завданням цієї мережі координаційних рад стане забезпечення вирішення конкретних організаційно-технічних питань щодо формування інформаційної і кібербезпеки окремих галузей та сфер життєдіяльності суб'єктів інформаційно-комунікаційних технологій для зміцнення загального рівня національної безпеки (рис. 3.3).

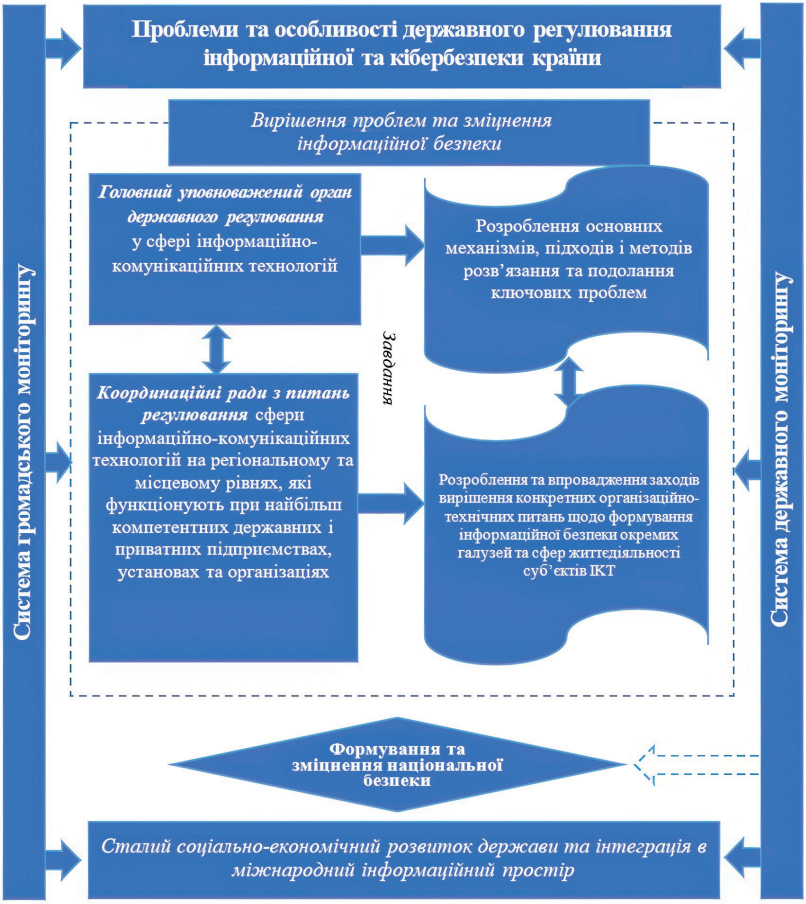

Рис. 3.3. Механізм вирішення проблем державного регулювання у сфері інформаційно-комунікаційних технологій

Як ми бачимо, важливе місце в запропонованому механізмі вирішення проблем державного регулювання у сфері інформаційно-комунікаційних технологій посідає система громадського та державного моніторингу.

Мета створення такої системи моніторингу полягає в здійсненні постійного контролю з боку громадськості та уповноважених державних органів за ефективним впровадженням та реалізацією нормативно-правових інститутів державного регулювання сфери інформаційно-комунікаційних технологій.

Крім того, специфіка сучасного соціально-економічного розвитку України диктує необхідність створення самостійної системи моніторингу корупційної діяльності, який визначить найбільш важливі напрямки антикорупційних програм, дозволить оцінити їхню ефективність і своєчасно їх скорегувати. Зазначимо, що саме корупційна складова часто породжує найбільш значні порушення у сфері користування та застосування інформаційно-комунікаційних технологій та є ключовою загрозою національній безпеці крайні.

Виходячи із цього, для вирішення завдання моніторингу корупційної діяльності можна запропонувати такі заходи: дослідити загальноприйняті корупційні практики та впроваджувати їх у нормативно-правовій практиці України; відстежити механізми корупційних угод та розробити механізми щодо запобігання їм; визначити рівень та структуру корупційної діяльності та розробити стратегічні положення щодо зниження цього рівня; проаналізувати фактори, що сприяють корупційній діяльності, та вдосконалити механізми виявлення й усунення цих факторів; здійснювати комплексний контроль за ефективністю реалізації антикорупційних програм.

Таким чином, розроблення системи моніторингу результативності державного регулювання сфери інформаційно-комунікаційних технологій дозволить оцінити хід впровадження нормативно-правових інститутів, визначити, наскільки досягнуто поставлені цілі та отримано заплановані показники результативності. Основні результати успішно вибудованої системи громадського та державного моніторингу:

1. Своєчасна і достовірна оцінка та загальне сприйняття інформаційним суспільством заходів щодо державного регулювання сфери інформаційно-комунікаційних технологій шляхом організації публічних обговорень основних напрямів цього регулювання, що, у свою чергу, забезпечить інформаційну та експертно-методологічну підтримку його успішної реалізації.

2. Здійснення ефективних та комплексних реформ у сфері інформаційної та кібербезпеки суб'єктів інформаційно-комунікаційних технологій.

3. Підвищення відкритості діяльності органів державного управління та місцевого самоврядування в цілому за рахунок використання сучасних інформаційно-комунікаційних технологій.

4. Розроблення та впровадження об'єднаної бази даних щодо регулювання сфери та суб'єктів інформаційно-комунікаційних технологій.

5. Створення механізмів, за допомогою яких можна оцінити ефективність державного регулювання інформаційно-комунікаційної сфери окремими органами регіональної та місцевої влади для забезпечення мотивації та фінансової підтримки впровадження цих заходів.

6. Формування та зміцнення національної безпеки країни як в інформаційній сфері, так і в інших галузях шляхом впровадження дієвих механізмів захисту інформацій та комунікації.

Отже, комплексна та дієва система державного регулювання сфери інформаційно-комунікаційних технологій є ключовим напрямом функціонування влади на всіх рівнях – від державного до місцевого та передбачає низку заходів нормативно-правового, технологічного, технічного, програмного, соціально-економічного і політичного характеру, успішне впровадження яких розкриє широкі горизонти реалізації ідей демократичного інформаційного суспільства і правової держави, а також дозволить зміцнити всі напрями національної безпеки країни.

3.2. Концептуальні основи побудови системи національної кібербезпеки

Першим документом, що визначає стратегію нашої держави у сфері кібербезпеки, став Указ Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року № 96/2016 «Про Стратегію кібербезпеки України», у якому було визначено такі основні завдання:

- розвиток безпечного, стабільного та надійного кіберпростору;
- кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації;
- кіберзахист критичної інфраструктури;
- розвиток потенціалу сектора безпеки та оборони у сфері забезпечення кібербезпеки;
- боротьба з кіберзлочинністю.

Згідно з Указами Президента України № 8/2017, № 32/2017 та № 254/2017 введено в дію рішення Ради національної безпеки і оборони України (РНБО) «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», «Про заходи забезпечення захисту об'єктів критичної інфраструктури та заходи щодо нейтралізації кіберзагроз», «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

5 жовтня 2017 року було прийнято Закон «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року. Цей закон є основоположним нормативно-правовим актом у сфері забезпечення кібербезпеки держави, який:

- визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України в кіберпросторі;
- структурує положення про національну систему кібербезпеки;
- вводить механізми застосування сучасних європейських практик і стандартів;
- розподіляє функції між правоохоронними органами та спецслужбами щодо забезпечення кібербезпеки.

Закон також визначає основних суб'єктів забезпечення кібербезпеки України: ДССЗЗІ України, СБУ, МВС України, Міністерство оборони України, розвідувальні органи України, НБУ.

За стратегічне управління та координацію роботи відомств, що забезпечують кібербезпеку, відповідає РНБО [7]. Їй підпорядкована ДССЗЗІ, що розробляє комплексну систему кіберзахисту стратегічних об'єктів та опікує компанії, які проводять аудит стратегічних об'єктів. ДССЗЗІ підпорядкований Державний центр кіберзахисту та протидії кіберзагрозам, підрозділ якого – Оперативний центр реагування на кіберінциденти здійснює моніторинг і виявляє потенційні кіберзагрози (рис. 3.4).

Кіберзахистом також займаються: МВС України, яке відповідає за запобігання кіберзлочинам та їхнє розслідування; МОУ і Генеральний штаб (ГШ) ЗСУ, що забезпечують охорону військових об'єктів та об'єктів критичної інфраструктури під час війни та в період надзвичайного стану; СБУ, яка має запобігати терористичним атакам у кіберпросторі та яку наділено правом перевіряти об'єкти критичної інфраструктури, перелік яких визначає Кабінет Міністрів; кібербезпека в банківській сфері – зона відповідальності НБУ.

Власники об'єктів критичної інфраструктури вважаються виконавцями державної політики кібербезпеки, тобто зобов'язані впрова-

джувати її на своєму підприємстві. Якщо державні установи, включаючи міністерства, стануть об'єктом кіберзлочинців, відповідальність буде нести керівництво цих установ. Чиновники нарешті усвідомили, що різні галузі економіки та сфери життєдіяльності України стають дедалі більш вразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Слід зауважити, що зловмисники прямо чи опосередковано пов'язані з рф.

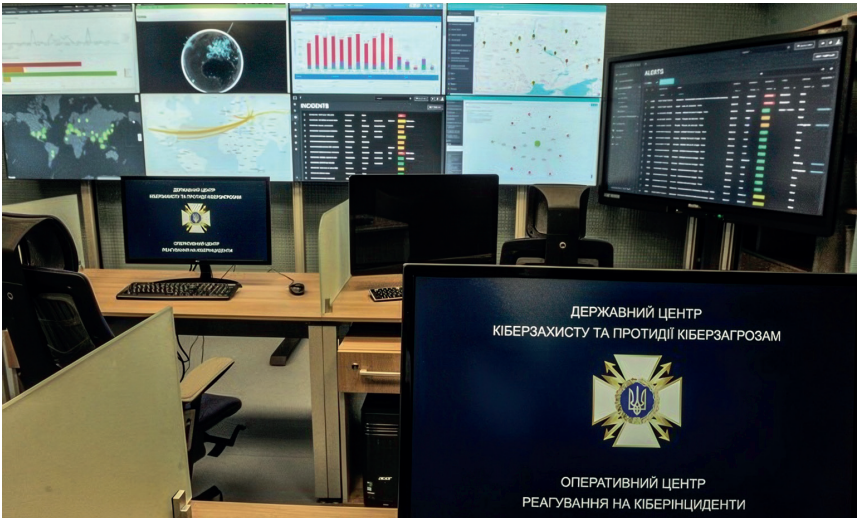

Рис. 3.4. Державний центр кіберзахисту та протидії кіберзагрозам

Як бачимо, повноваження органів, що відповідають за кібербезпеку, частково перетинаються, тому спробуємо точніше визначити, який орган і за що саме відповідає.

ДССЗЗІ відповідає за технічний захист інформації, криптозахист даних, що є власністю держави, та захист персональних даних. Ця служба ліцензує компанії, які мають право надавати послуги криптозахисту та технічного захисту інформації, видає атестати відповідності на засоби та комплексні системи захисту інформації. При ДССЗЗІ є Центр реагування на кіберзагрози для ресурсів держави – CERT.UA (підрозділ, який структурно належить до Державного центру кіберзахисту та протидії кіберзагрозам). На нього покладено функції попередження кібератак та ліквідації їхніх наслідків. При ДССЗЗІ також працює Центр антивірусного захисту інформації, який відповідає за захист інформаційних ресурсів держави.

СБУ відповідає за захист інтересів держави та прав громадян в інформаційному середовищі. В СБУ створено Ситуаційний центр забезпечення кібернетичної безпеки на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки цього відомства. Завдання Центру – запобігання хакерському втручанню в роботу об'єктів критичної інфраструктури та державних служб. Центр має власну лабораторію комп'ютерної криміналістики та реагування на кіберінциденти.

Підрозділом МВС України є кіберполіція, яка веде розслідування у сфері розміщення протиправного контенту в Інтернеті, злому платіжних систем і майданчиків e-commerce. Цей підрозділ також зобов'язаний інформувати громадян про нові загрози та протидіяти їхньому поширенню.

У МОУ теж є підрозділи, що відповідають за інформаційну безпеку. Спеціальні заходи щодо забезпечення національних інтересів в інформаційній сфері організовує і проводить Головне управління розвідки (ГУР) МОУ, а також Служба зовнішньої розвідки (СЗР) України.

Створено Центр кіберзахисту при НБУ для реагування на кіберінциденти в банківській системі України та аналогічний центр при Міністерстві інфраструктури – Галузевий центр цифровізації та кібербезпеки (ГЦЦК).

Отже, основою системи національної кібербезпеки є центри виявлення, управління та реакції на кіберзагрози [8]. У світовій практиці існує декілька термінів на позначення таких центрів: CERT, CSIRT (Computer Security Incident Response Team), SOC (Security Operation Center). Так, національні центри протидії кіберзагрозам майже завжди називають CERT. Ці центри створено державними структурами для боротьби з кіберзагрозами, спрямованими на державні органи управління та інші критично важливі об'єкти, або з кіберзагрозами державного масштабу. В Україні таких центрів два: CERT-UA в ДССЗЗІ, а також центр рівня CERT в СБУ. Такі центри є ядром системи кібербезпеки держави, вони взаємодіють у системі міжнародного обміну інформацією про кіберзагрози, шкідливі активності та тренди атак.

Крім центрів національного масштабу, система кібербезпеки держави включає галузеві команди реагування на комп'ютерні надзвичайні події (CSIRT). Такі команди рекомендовано створювати в кожній галузі, особливо, якщо галузь має велику кількість об'єктів критичної інфраструктури. Саме на ці центри покладено завдання реагувати на кіберінциденти на підприємствах критичної інфраструктури галузі, відповідно до постанови Кабінету Міністрів України № 518 від 19 червня 2019 року

«Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Цей документ визначає організаційно-методологічні, технічні й технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесено до об'єктів критичної інфраструктури. Загалом такі галузеві центри кібербезпеки покликані виявляти кіберзагрози на підприємствах галузі, реагувати на них та взаємодіяти з національними CERT.

Наступним рівнем системи кібербезпеки є центри управління кібербезпекою окремих організацій, державних чи комерційних підприємств, зокрема інфраструктурних та фінансових установ, різноманітних об'єднань, підприємств та ін. Такі центри управління кібербезпекою називають SOC. Вони покликані виявляти, локалізувати загрози та реагувати на кіберінциденти на окремому підприємстві, в організації, корпорації чи холдингу. Перевагою SOC є максимальна заглибленість в IT-інфраструктуру конкретного підприємства, тобто можливість швидко розібратися в сутності інциденту й локалізувати його наслідки. Тому такі центри є найбільш ефективними для боротьби з кіберзагрозами для підприємств, у яких кількість користувачів перевищує 500, а також для тих, які зберігають чи обробляють інформацію, втрата або виток якої будуть критичними для підприємств та організацій або держави.

Ще одним компонентом системи кібербезпеки є комерційні SOC, що надають послуги з виявлення кіберзагроз та кіберінцидентів і, за можливості, реагування на них для підприємств, які розуміють важливість забезпечення кібербезпеки, але з якихось причин не створюють свій SOC, а отримують ці послуги із хмари оператора. Такі оператори називаються MSSP (Managed Security Service Provider) або MDR (Managed detection and response). Такі комерційні центри можуть взаємодіяти з CERT національного рівня після перевірки щодо виконання вимог та умов взаємодії з точки зору забезпечення національної безпеки.

Використовуючи системний підхід [9], який полягає в застосуванні сукупності методологічних принципів і теоретичних положень, що дають змогу розглядати кожний елемент системи в його зв'язку і взаємодії з іншими елементами; простежувати зміни, що відбуваються в системі в результаті зміни окремих її ланок; вивчати специфічні системні (емерджентні) властивості; робити обґрунтовані висновки про закономірності розвитку системи; визначати оптимальний режим її функціонування [10], можна побудувати модель системи національної кібербезпеки у вигляді трирівневої піраміди (рис. 3.5).

В основу моделі покладено концепцію єдиного інформаційного простору для обміну даними про кіберінциденти як усередині країни, так і за її межами, і такі принципи [11]:

- принцип цілісності – розгляд водночас системи як єдиного цілого та як підсистеми для вищих рівнів;
- принцип ієрархічності – наявність безлічі елементів, розташованих на основі підпорядкування елементів нижчого рівня елементам вищого рівня;
- принцип структуризації – аналіз елементів системи та їх взаємозв'язку в рамках конкретної організаційної структури;
- принцип множинності – використання безлічі кібернетичних, економічних і математичних моделей для опису окремих елементів і системи в цілому;
- принцип системності – володіння об'єктом усіх ознак системи.

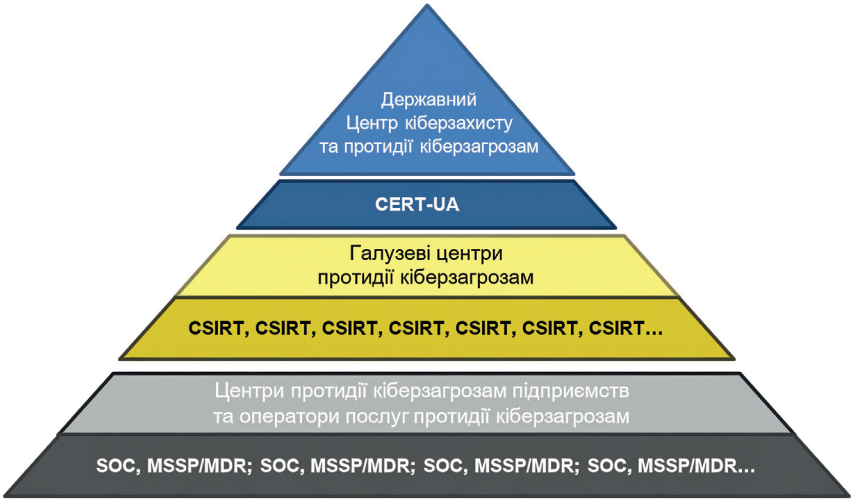

Рис. 3.5. Модель системи національної кібербезпеки

Для підвищення ефективності боротьби з кіберзагрозами на рівні країни організовано взаємодію центрів та обмін інформацією про виявлені кіберінциденти, особливо якщо вони викликані невідомими раніше кіберзагрозами. У цих випадках якнайшвидше поширення такої інформації та внесення до бази індикаторів компрометації (Indicators of Compromise, IoC) правил кореляції та реакції кожного центру боротьби з кіберзагрозами є принципово важливими для запобігання масовим ата-

кам і порушенням у роботі інформаційно-технологічної інфраструктури державних установ та відомств.

Модель взаємодії центрів протидії кіберзагрозам та обміну інформацією між ними подано на рис. 3.6. Ядром цієї моделі є центри національного рівня CERT, які здійснюють обмін інформацією про загрози (IoC) з подібними національними та міжнародними центрами. CERT національного рівня є центром збирання, аналізу, обробки, зберігання та обміну інформацією про загрози в країні. CERT також узгоджує протокол взаємодії й обміну інформацією в національній мережі та вимоги для підключення центрів до цієї мережі.

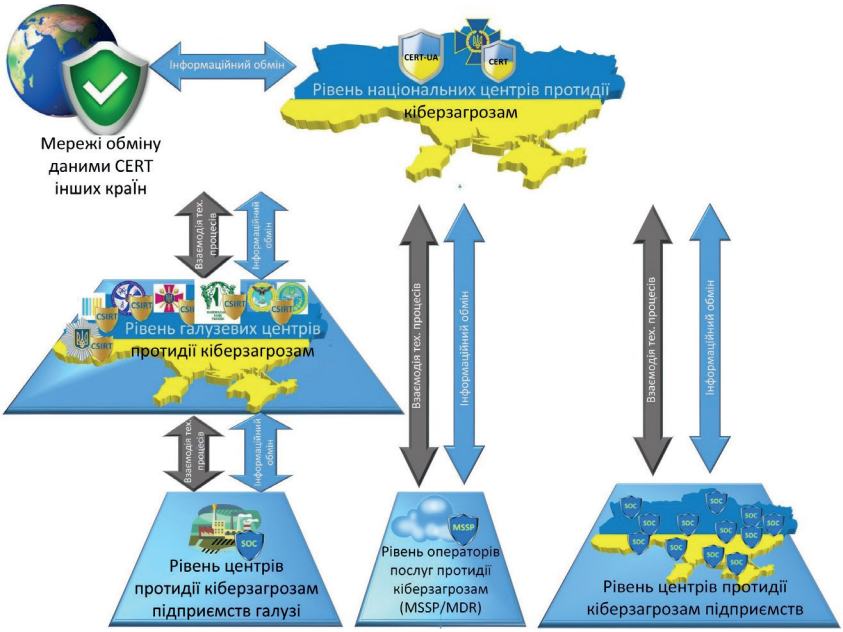

Рис. 3.6. Модель взаємодії центрів протидії кіберзагрозам та обміну інформацією

CSIRT галузевого рівня здійснюють обмін інформацією безпосередньо із центрами національного рівня. Підприємства галузі, які мають власний SOC, є третім рівнем системи національної кібербезпеки. Вони підключаються до національної мережі обміну інформацією з кібербезпеки через CSIRT відповідної галузі, якщо такий є, і безпосередньо із центром національного рівня CERT, якщо CSIRT галузі не функціонує.

SOC окремих підприємств, корпорацій та холдингів також взаємодіє безпосередньо із центром національного рівня CERT, підключається до мережі згідно із затвердженими протоколами взаємодії після виконання відповідних вимог.

Підключення до національної мережі для обміну інформацією щодо кібербезпеки операторів, які надають послуги SOC, здійснюється за тими самими принципами, що й підключення SOC підприємств, але перед тим потрібно провести аналіз і контроль усіх замовників їхніх послуг, тому що такі оператори можуть надавати послуги організаціям та установам різних країн.

Отже, зважаючи на те, що останнім часом розвідувально-підривна діяльність іноземних спецслужб у кіберпросторі посилюється, систему кіберзахисту в Україні необхідно розвивати та вдосконалювати з урахуванням рівня сучасних загроз. Державним організаціям, що відповідають за кіберзахист, треба постійно актуалізувати вимоги щодо кіберзахисту, яких мають дотримуватися всі об'єкти критичної інфраструктури; визначити повний список таких об'єктів й уточнювати його в разі потреби. Керівникам цих об'єктів необхідно впроваджувати досить надійну систему кіберзахисту з урахуванням усіх вимог.

Не можна забувати про захист і керівникам підприємств та організацій, які не входять до переліку об'єктів критичної інфраструктури. Слід пам'ятати, що захист від кіберзагроз тепер стосується кожного, отже, варто подбати про нього і пересічним громадянам.

Висновки до третього розділу

У системі формування та зміцнення національної безпеки України визначальну роль відіграє ефективне державне регулювання у сфері інформаційно-комунікаційних технологій, інформаційної та кібербезпеки. Комплексна та дієва система державного регулювання сфери інформаційно-комунікаційних технологій є ключовим напрямом функціонування влади на всіх рівнях – від державного до місцевого та передбачає низку заходів нормативно-правового, технологічного, технічного, програмного, соціально-економічного та політичного характеру, успішне впровадження яких розкриє широкі горизонти реалізації ідей демократичного інформаційного суспільства і правової держави, а також дозволить зміцнити всі напрями національної безпеки країни.

Основою системи національної кібербезпеки є центри виявлення, управління та реакції на кіберзагрози. Такі національні центри про-

тидії кіберзагрозам майже завжди називають CERT. Вони створені державними структурами для боротьби з кіберзагрозами, спрямованими на державні органи управління та інші критично важливі об'єкти, або з кіберзагрозами державного масштабу. В Україні таких центрів два: CERT-UA – в ДССЗЗІ, а також центр рівня CERT – в СБУ. Ці центри є ядром системи кібербезпеки держави. Вони взаємодіють у системі міжнародного обміну інформацією про кіберзагрози, шкідливі активності та тренди атак.

Для підвищення ефективності боротьби з кіберзагрозами на рівні країни потрібно організувати взаємодію центрів та обмін інформацією про виявлені кіберінциденти. Якщо вони викликані невідомими раніше кіберзагрозами, то в цих випадках якнайшвидше поширення такої інформації та внесення до бази індикаторів компрометації правил кореляції та реакції кожного центру боротьби з кіберзагрозами є принципово важливими для запобігання масовим атакам і порушенням у роботі інформаційно-технологічної інфраструктури державних установ та відомств.

Запропоновано модель взаємодії центрів протидії кіберзагрозам та обміну інформацією. Ядром цієї моделі є центри національного рівня CERT, які здійснюють збирання, аналіз, обробку, зберігання та обмін інформацією про загрози в країні з подібними національними та міжнародними центрами, а також узгоджують протокол взаємодії й обміну інформацією в національній мережі та вимоги для підключення центрів до цієї мережі.

Перелік використаних джерел:

1. Лисецький Ю. М. Концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки. *Вісник воєнної розвідки*. 2023. № 75. С. 33–36.

2. Yurii Lysetskyi, Yurii Semenyuk, Giuseppe T. Cirella, Dmytro Pavlenko, Gevorkyan A. Yuriyovich, Oleh Demydkin. Conceptual Framework of Ukraine's National Security: Regulatory Examination Using Information and Communication Technologies. Handbook on Post-War Reconstruction and Development Economics of Ukraine, 2024. Pages 31–46.

3. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету : серія «Право».* № 42. 2017. С.16–22.

4. Лисецький Ю. М. Інформаційні технології в управлінні та обробці інформації: монографія. Київ : ЛАТ&К, 2018. 268 с.

5. Сопілко І. М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. *Юридичний вісник*. 2017. № 3(44). С. 61–64.

6. Грохольський В. Л. Визначення сутності державного управління та його відмежування від суміжних понять. *Інтернаука*. Серія : «Юридичні науки». 2017. № 1 (1). С. 28–32.

7. Лисецький Ю. М., Бобров С. І. Деякі аспекти побудови системи національної кібербезпеки. *Математичні машини і системи.* 2021. № 2. С. 15–22.

8. Лисецький Ю. М., Крисяк П. В. Концептуальні основи системи національної кібербезпеки. *Вісник воєнної розвідки*. 2021. № 65. С. 67–72.

9. Блауберг И. В., Садовский В. Н., Юдин Э. Г. Системный подход в современной науке. Проблемы методологии системных исследований. М. : Мысль, 1970. С. 7–48.

10. Берталанафи Л. История и статус общей теории систем. М : Наука, 1973. 364 с.

11. Вентцель Е. С. Исследование операций: задачи, принципы, методология. М. : Наука, 1988. 206 с.

РОЗДІЛ 4
МЕТОДИ ТА СПОСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

4.1. Існуючі підходи до забезпечення інформаційної та кібербезпеки

На сьогоднішній день серед вітчизняних організацій можна виділити такі підходи до забезпечення інформаційної та кібербезпеки: ситуаційний, інтеграційний та інтеграційно-інноваційний [1].

Ситуаційний підхід характерний для організацій, у яких збереження інформації не впливає безпосередньо на їхнє функціонування. Відмінними рисами ситуаційного підходу є точкове впровадження систем безпеки і відсутність централізації управління інформаційною безпекою. Наприклад, під час розгортання нової CRM-системи (Customer Relationship Management) фахівці з впровадження самі визначають механізми захисту нової системи. IT-фахівці на свій розсуд обирають методи захисту, наприклад, PAM (Privileged Access Management), DLP (Data Loss Prevention), 2FA (Dual Factor Authentication), а після впровадження – приймають весь комплекс в експлуатацію. Таким чином, фахівці з БД відповідають за безпеку БД, фахівці із систем зберігання даних (СЗД) – за захист СЗД, фахівці з ПЗ – за безпеку свого ПЗ. У таких умовах кожен структурний підрозділ організації формує свої правила безпеки, власну політику надання доступу співробітникам, роботи з паролями, відстеження параметрів роботи обладнання, регулярного резервного копіювання тощо. При цьому завдання з регулярного сканування IT-інфраструктури, відстеження актуальності версій використовуваного ПЗ, контролю вірусної активності, як правило, залишаються без належної уваги фахівців або віддаються «на відкуп» локальним адміністраторам.

Отже, ситуаційний підхід вирізняється інертністю й незлагодженістю систем захисту та забезпечення інформаційної та кібербезпеки організації, відсутністю системного планування розвитку IT-інфраструктури, що негативно впливає на планування розвитку систем інформаційної та кібербезпеки організації загалом. Тому ситуаційний підхід може бути застосовний тільки для невеликих оргагізацій (100–200 співробітників) з єдиною IT-службою, яка обслуговує всю IT-інфраструктуру. У разі

збільшення масштабів організації або поділу ІТ-служби за напрямками (мережа, сервери, БД, ПЗ, оптична мережа, системи автоматизації тощо) організації необхідно переглянути свій підхід до забезпечення інформаційної та кібербезпеки та трансформувати його в інтеграційний.

Інтеграційний підхід – це наступний рівень забезпечення інформаційної та кібербезпеки організації. Він характеризується наявністю виділених служб планування і забезпечення роботи систем інформаційної та кібербезпеки організації, формуванням єдиних вимог до таких систем, аналізом критичності інформаційних активів і потенційних загроз, їх залежністю від функціональних процесів організації.

Інтеграційний підхід має на увазі насамперед розроблення вимог до забезпечення безпеки ІТ-інфраструктури та даних з урахуванням архітектури філіальної мережі, особливостей хмарних сервісів, унікальними потребами персоналу і контрагентів. При цьому першим важливим кроком розроблення цих вимог є визначення та розуміння ландшафту кіберзагроз, можливих напрямків атак і потенційних проблем під час роботи з критичною інформацією.

Застосування інтеграційного підходу до забезпечення інформаційної та кібербезпеки організації дає змогу передбачити потенційні загрози та вектори атак, знизити ризик витоку та пошкодження даних, зменшити час простою сервісу під час відновлення. Середні та великі організації мають велику та комплексну ІТ-інфраструктури, що, своєю чергою, значно збільшує периметр безпеки. Великі масштаби вимагають також нових механізмів забезпечення інформаційної та кібербезпеки.

Інтеграційно-інноваційний підхід до забезпечення інформаційної та кібербезпеки застосовують організації корпоративного рівня, які будують SOC, Центри оперативного реагування на кіберінциденти (ЦОРК) або системи забезпечення інформаційної та кібербезпеки [2–4]. Такі централізовані системи моніторингу інформаційної та кібербезпеки в автоматичному режимі відстежують показники роботи різних елементів ІТ-інфраструктури, а застосування штучного інтелекту підвищує ефективність забезпечення інформаційної та кібербезпеки організації в цілому [5]. Окремим напрямком у рамках інтеграційно-інноваційного підходу є розроблення процедур забезпечення безперервності функціонування (Business Continuity Plan, BCP) і плану відновлення після збою (Disaster Recovery Plan, DRP) [6, 7]. Організації, які розробили такі процедури, забезпечують завчасну підготовку до негативних сценаріїв порушення роботи ІТ-інфраструктури.

Отже, основні відмінності розглянутих підходів до забезпечення інформаційної та кібербезпеки подано на рис. 4.1.

Нині, незалежно від підходу до забезпечення інформаційної та кібербезпеки, організації стикаються з аналогічними проблемами під час вибору методів і технологій захисту інформації.

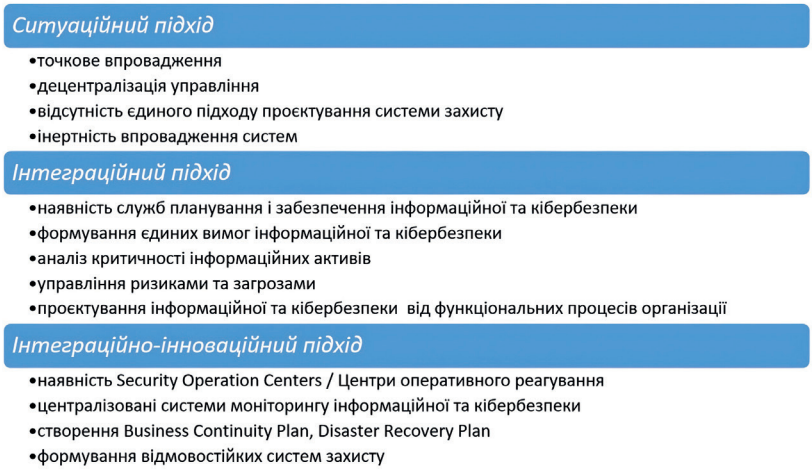

Рис. 4.1. Відмінності підходів до забезпечення інформаційної та кібербезпеки організації

По-перше, це нестача фахівців у галузі кібербезпеки, що створює додаткові ризики піддатися кібератакам із порушенням роботи сервісів або витоком даних. Дуже важливою складовою системи інформаційної та кібербезпеки є персонал.

Основними вимогами до персоналу, що відповідає за інформаційну та кібербезпеку, є: знання інструментів безпеки хмарних і серверних платформ, симптомів атак і загроз, критичних функціональних процесів для організації.

На тлі постійного зростання й ускладнення IT-інфраструктури ефективність процесів оновлення прошивок операційних систем і версій ПЗ, що використовується, знижується внаслідок недостатньої систематизації та автоматизації цих завдань, що зі свого боку не дає змоги забезпечувати необхідний рівень інформаційної та кібербезпеки організації.

По-друге, периметр корпоративної мережі «розмився» в результаті впровадження віддалених / мобільних робочих місць і технологій

BYOD (Bring Your Own Device) [8]. Поступова міграція в хмарні технології, з появою некерованих користувацьких мобільних пристроїв, ускладнює захист інфраструктури організації, вимагає впровадження відповідних політик управління та обліку мобільних пристроїв, а операційне середовище організації – багатофакторної аутентифікації та шифрування даних.

По-третє, недостатня увага до тонкого налаштування міжмережевих екранів (ММЕ), які забезпечують доступ користувачів до ІТ-інфраструктури та захист від неавторизованого доступу. Завдання ускладнюється, оскільки частина сервісів, користувачів і даних перебуває за ММЕ у хмарі, що збільшує ризик витоку інформації та безпеки використання особистих пристроїв і ПЗ.

Проблему тонкого налаштування частково вирішують ММЕ нового покоління NGFW (Next-Generation Firewall) і SIEM (Security Information and Event Management) системи [9, 10]. NGFW, об'єднуючи в собі антивірусний захист, перевірку шифрованого трафіку і трафіку на різних рівнях OSI-моделі (Open Systems Interconnection model), вебфільтр, контроль доступу на основі DNS (Domain Name System), запобігання вторгненням й антиспам, спрощує завдання контролю ключових точок периметра інформаційної безпеки [11, 12]. А інтеграція NGFW з технологіями і пристроями програмно-керованих мереж – SD-WAN (Software Defined Wide Area Network) являє собою ще більш ефективний інструмент для застосування в розподілених мережах [13].

SIEM-системи, з поширенням хмарних технологій, стали доступнішими та дешевшими. Відповідно більшість організацій із розвиненою ІТ-інфраструктурою вже знайомі з роботою SIEM на практиці. Проте ефективність SIEM-системи в першу чергу залежить від розуміння ІТ-службою вимог до інформаційної та кібербезпеки і правильного налаштування кореляційних правил для ефективного виявлення релевантних загроз. Функціонал SIEM-системи подано на рис. 4.2.

Широке застосування хмарних технологій призвело до появи нових векторів атак і відповідно нових викликів для наявних систем інформаційної та кібербезпеки. Поширення набули публічні та гібридні моделі розгортання хмар. Однак окрім традиційних загроз (втрата та витік даних; несанкціонований доступ; неналежний контроль за правами доступу) додаються нові загрози: небезпечних інтерфейсів та API (Application Programming Interface); неправильне налаштування хмарної платформи. Що стосується інструментів і платформ забезпечення інформаційної та кібербезпеки у хмарі, то наявність віртуалізації та різ-

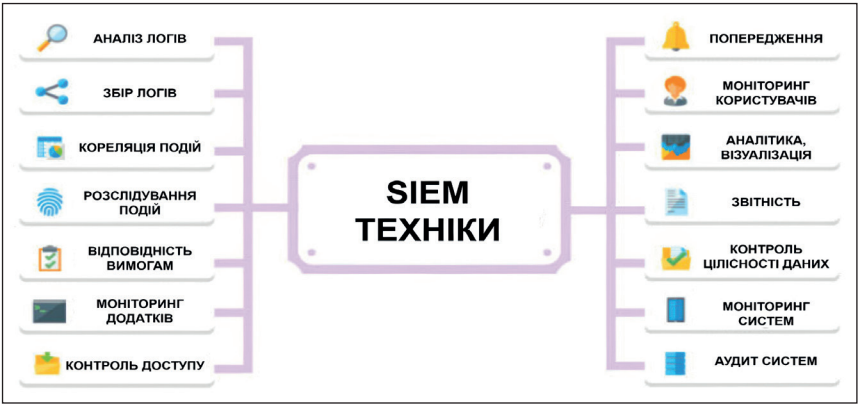

Рис. 4.2. Функціонал SIEM-системи

номанітних сервісних моделей хмарних обчислень призвела до появи нових, специфічних, але водночас більш продуктивних і масштабованих інструментів захисту.

При цьому основними специфічними функціями забезпечення інформаційної та кібербезпеки у хмарі є: перевірка достовірності та авторизація; захист даних і запобігання їхньому витоку; забезпечення всебічної видимості функціональних сервісів і блокування роботи несанкціонованого ПЗ. Цією функціональністю володіє сервіс CASB (Cloud Access Security Broker) – брокер безпеки хмарного доступу, який об'єднує в собі функції IAM-системи (Identity and Access Management) перевірки аутентичності, хмарного брандмауера, безпечного вебшлюзу – WAF (Web Application Firewall)) і DLP-системи запобігання втраті даних [14–16]. Використання CASB в галузі інформаційної та кібербезпеки дозволяє вирішувати такі завдання (рис. 4.3):

• *Контроль доступу*: CASB забезпечує контроль над доступом до хмарних сервісів, додатків та даних. Він дозволяє визначати та управляти політиками доступу, аутентифікацією, авторизацією та аудитом, щоб запобігти несанкціонованому доступу та керувати привілеями користувачів.

• *Захист даних*: CASB забезпечує механізми захисту даних у хмарі. Він може застосовувати шифрування даних, контролювати та запобігати витоку інформації, виявляти та запобігати шкідливим атакам, забезпечувати безпечне зберігання та передачу даних.

• *Виявлення та реагування на загрози*: CASB надає можливості виявлення та моніторингу аномальної активності й потенційних загроз

безпеці в хмарних сервісах. Він може попереджувати про підозрілі дії, пропонувати алгоритми реагування та вживати заходів для пом'якшення загроз.

• *Відповідність регуляторним вимогам*: CASB допомагає організаціям дотримуватися регуляторних вимог та стандартів у галузі інформаційної безпеки. Він надає інструменти для контролю та звітності, а також допомагає встановлювати відповідні політики та процедури.

• *Моніторинг та аудит*: CASB надає можливість моніторингу та аудиту дій користувачів, доступу до даних та подій у хмарних сервісах. Він реєструє та аналізує активність, дозволяючи організаціям відстежувати та ідентифікувати потенційні проблеми безпеки.

• *Управління політиками безпеки*: CASB дозволяє визначати та застосовувати політики безпеки в хмарних середовищах. Він надає засоби для встановлення та управління політиками, правилами та обмеженнями, щоб забезпечити відповідність внутрішнім вимогам організації та встановити узгоджену безпеку в хмарі.

Рис. 4.3. Завдання, які вирішує CASB

Основні тенденції розвитку IT-інфраструктури наразі сфокусовані в напрямку хмарних технологій. Відповідно, вже сьогодні та в найближчому майбутньому будуть актуальними завдання забезпечення безпечної взаємодії «наземної» частини IT-інфраструктури з хмарною, інтеграцію систем авторизації хмарних і наземних інфраструктур, витоку інформації з хмарних СЗД.

Отже, розглянувши підходи до забезпечення інформаційної та кібербезпеки вітчизняних організацій, можна зробити висновок, що інформаційна та кібербезпека має ґрунтуватися на комплексному підході та ефективній інтеграції всіх елементів IT-інфраструктури на різних рівнях їхньої взаємодії. Це зумовлено впровадженням нових методів організації роботи в організаціях, передових IT-технологій, повсюдної автоматизації та цифровізації, розповсюдженням хмарних технологій, BYOD, SD-WAN, IoT. Додаткові вимоги до забезпечення інформаційної та кібербезпеки також диктуються регуляторною політикою держави та галузевими стандартами. Водночас виникає необхідність розроблення стратегій захисту та впровадження систем управління кібербезпекою, що дають змогу оперативно реагувати на кіберзагрози, контролювати інформаційний периметр організації та керувати потоками даних в IT-інфраструктурі.

4.2. Організаційно-технічні методи підвищення рівня кіберзахисту IT-систем

Поступово, з часу організації Інтернету і до наших днів, кіберпростір як мережа для обміну інформацією перетворився на інструмент впливу на реальність, у якій дії окремих хакерів та/або кіберугруповань можуть призвести до цілком реальних втрат і катастроф. Так, атаки на комп'ютерні системи диспетчерського управління і збирання даних (Supervisory Control And Data Acquisition, SCADA) технологічними процесами підприємств і системи управління енергетичними мережами є постійною загрозою для цих систем у всьому світі. Проте під загрозою не лише ці системи. За допомогою IT та кібератак злочинні угруповання і спецслужби намагаються втручатись у політичні та економічні процеси інших країн. Наведемо деякі приклади.

1982 рік. Діяльність кіберпідрозділу ЦРУ (Центральне розвідувальне управління) США проти шпигунської діяльності Комітету державної безпеки Союзу Радянських Соціалістичних Республік. Унаслідок втручання шкідливого програмного забезпечення (ШПЗ) сталися помилки в роботі програми керування технологічними процесами, що призвело до потужного вибуху на ділянці газопроводу Уренгой – Сургут.

2008 рік. Діяльність кіберпідрозділу ЦРУ та Моссад проти Іранського центру збагачення урану. За допомогою вірусу Stuxnet в Ірані було зруйновано тисячі центрифуг на виробництві збагаченого урану компанії Siemens, що призвело до уповільнення реалізації ядерної програми на декілька років та значних фінансових втрат.

2015 рік. Діяльність хакерського угруповання Sandworm, а фактично кіберпідрозділу Головного розвідувального управління (ГРУ) ГШ рф на енергетичну мережу України. Системи SCADA зазнали атаки ШПЗ BlackEnergy3, що призвело до тимчасового припинення електропостачання для великої кількості споживачів трьох компаній «Обленерго».

2016 рік. Здійснено хакерську атаку на ІС та окремі поштові сервери демократичної партії з метою компрометації одного з кандидатів під час президентських виборів у США. 2018 року міністерство юстиції США висунуло звинувачення проти 12 російських військових із ГРУ ГШ рф за спробу втручання росії в перебіг виборів 2016 року.

2017 рік. Вірус CrashOverride, також відомий як Industroyer, було використано для атаки на електроенергетичні системи в Україні. Це перше відоме ШПЗ, спеціально розроблене для атаки на системи управління енергетичними мережами.

2017 рік. Атака за допомогою вірусів WannaCry та NotPetya на український корпоративний сектор, що призвела до великих фінансових та репутаційних збитків.

2023 рік. Хакерська атака на оператора мобільного зв'язку «Київстар», відповідальність за яку взяло на себе російське хакерське угруповання «Солнцепёк», що тісно пов'язане з Sandworm та ГРУ ГШ рф. Під час атаки хакери дістали доступ до ключових вузлів ІТ-інфраструктури «Київстар» – контролера домену та сервісів віртуалізації, які в подальшому було видалено, що призвело до збою в роботі транспортної мережі та унеможливило надання компанією сервісів своїм замовникам. По всій країні в більше ніж 24 мільйонів абонентів «Київстар» зник мобільний зв'язок та Інтернет, до того ж користувачі не могли приєднатися до мереж інших операторів у рамках внутрішнього українського роумінгу. Збої сталися в роботі всього обладнання, яке використовувало зв'язок через оператора «Київстар», що призвело до серйозних інфраструктурних проблем на всій території України.

2024 рік. Здійснено наймасштабнішу за останній час зовнішню хакерську атаку на державні реєстри України. Було призупинено роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції. Через атаку на державні реєстри у «Дії» тимчасово стали недоступними 27 послуг, зокрема реєстрація ФОП та ТОВ, бронювання працівників від мобілізації, перереєстрація авто, реєстрація права власності на майно, оформлення допомоги дітям, «єОселя», «єВідновлення», подання заяв про шлюб та інші. Сервісні центри МВС також тимчасово призупинили надання окремих реєстраційних послуг, пов'язаних зі зміною власника транспортного засобу.

Усі ці атаки є яскравим проявом використання того, що зараз має назву «розвинена стійка загроза» (advanced persistent threat – APT) – різновид складних кібератак з метою отримання несанкціонованого доступу до IT-систем жертви та встановлення прихованого доступу до неї для використання або контролю в майбутньому [17].

Низка дослідників визначає APT (а не власне саму кібератаку чи різновид ШПЗ) як угруповання висококваліфікованих, добре оснащених хакерів, які проникають в IT-системи з метою виведення їх із ладу та/або викрадення інформації [18, 19]. Найчастіше джерелами APT є спецслужби чи установи, які фінансуються з державних бюджетів та мають цілі, що виходять далеко за межі звичайної кіберзлочинності [20]: військова розвідка, економічний саботаж, промислове шпигунство, фінансові махінації, політичні маніпуляції.

Описати алгоритм роботи APT можна за допомогою такого життєвого циклу (Lifecycle):

Крок 1. Вибір цілі – державні органи, що впливають на прийняття управлінських рішень, об'єкти критичної інфраструктури тощо.

Крок 2. Пасивна розвідка – збирання інформації про публічні сервіси компанії (web, mail, git, vpn тощо), засоби захисту IT-систем та користувачів через відкриті джерела (Open Source Intelligence, OSINT), корпоративні сайти / сервіси, соціальні мережі, такі як FB / LinkedIn та спеціалізовані сервіси на кшталт Shodan.io.

Крок 3. Активна розвідка – сканування сервісів на наявність вразливостей у ПЗ або архітектурі та організації IT-систем.

Крок 4. Аналіз добутої інформації та вибір вектору атаки.

Крок 5. Підбір інструментів (c2, вірусів та експлойтів), розроблення сценарію їхнього використання та створення необхідної IT-інфраструктури для проведення атаки.

Крок 6. Експлуатація вразливостей – використання експлойтів до знайдених уразливостей, відправлення фішингових листів або поштових повідомлень, або повідомлень у месенджерах, що містять вірус. Головне завдання зловмисників на цьому етапі – проникнення всередину IT-систем.

Крок 7. Горизонтальне просування в ураженій IT-систем з пошуком уразливих внутрішніх сервісів, створення та закріплення легального каналу, який не привертатиме увагу IT-спеціалістів або спеціалістів з інформаційної та кібербезпеки.

Крок 8. Вертикальне просування, головне завдання якого полягає в отриманні найвищого рівня привілеїв у системі та пошук і скачування таємної / конфіденційної інформації.

Крок 9. Використання отриманих можливостей.

Після досягнення результату алгоритм повторюється для виконання іншого завдання або спрямування на іншу ціль.

Головними інструментами атаки перш за все є соціальна інженерія – фішингові листи та повідомлення з вірусами, які зорієнтовано на непідготовленого та вразливого користувача, що за звичкою перейде за посиланням або відкриє «завірусований» документ на своєму комп'ютері. Є й інші чинники, що дають змогу зловмисникам дістати доступ всередину ІТ-систем. Серед них варто відзначити нескоординованість взаємодії між підрозділами ІТ та з інформаційної та кібербезпеки, що призводить до несвоєчасного оновлення ПЗ та ОС, чим можуть скористатися зловмисники.

Спеціалісти ДССЗЗІ виявили показову тенденцію надання переваги спробам повторних атак. Хакери повертаються до попередніх цілей, якими володіють, і використовують їх як плацдарм для подальшої експансії в інші пов'язані ІТ-системи. Такий підхід дає зловмисникам можливість стратегічного планування майбутніх операцій і прогнозування реакції захисників ІТ-систем. Заздалегідь знаючи про мережеву інфраструктуру, захисні заходи, ключовий персонал і моделі комунікації організації-жертви, нападники мають істотну перевагу, коли йдеться про повернення до цілей, скомпрометованих у минулому. Інший важливий аспект – це те, що є організації, які мають інформаційну, медійну, розвідувальну або іншу цінність для зловмисника, тож він усіляко намагається отримати чи повернути собі доступ до необхідних йому джерел інформації.

Протидіяти різноманітним видам сучасних кібератак і кіберзагроз можна, лише підвищуючи рівень кіберзахисту ІТ-систем. Кіберзахист можна поділити на дві основні складові: технічну та організаційну [21].

Технічна складова на практиці є більш об'ємною й містить сукупність технічних засобів апаратно-програмних та програмних, які захищають ІТ-системи в цілому та її окремі елементи від несанкціонованих дій користувачів та зовнішніх зловмисників. Це сукупність технічних рішень, головним завданням яких є можливість контролю адміністраторами кібербезпеки, легітимності процесу доступу, обробки, переміщення інформації уповноваженими користувачами, а в разі порушення – вжиття необхідних заходів для припинення порушення та унеможливлення його повтору в майбутньому. Зазвичай, незважаючи на всю складність технічних рішень, впровадити їх дещо простіше, ніж побудувати організаційну складову, яка буде адекватно описувати процес захисту під час обробки, переміщення та зберігання інформації різними групами користувачів.

Відповідно, організаційна складова описує, яким чином, до яких керівних та статутних документів, за допомогою яких технічних рішень, які спеціалісти будуть захищати ІТ-системи та від яких саме загроз [22]. Організаційна складова – це побудована ієрархічна система документів від загального – концепція кібербезпеки до конкретного – політики та інструкції на всі випадки порушення кібербезпеки, які можуть статися з ІТ-системою в цілому та окремими конкретними її елементами. Вона базується на нормах національного законодавства та міжнародних і національних стандартах захисту ІТ-систем та інформації. До організаційної складової кіберзахисту належить:

- стратегія реагування на інциденти – це розроблення плану реагування на інциденти, зокрема, швидке виявлення, ізоляція вірусів та відновлення;
- політика безпеки (розроблення та впровадження політик безпеки, визначення правил доступу до інформації під час її обробки, переміщення та зберігання, контроль над аутентифікацією та діяльністю користувачів в ІТ-системи);
- безпекова обізнаність (Security Awareness) – це проведення регулярних тренінгів та навчань для користувачів із питань кібербезпеки, щоб підвищити їхню обізнаність та сформувати навички, допомогти збільшити їхню «алертність» щодо потенційних загроз. Регулярні оновлення інструкцій та політики інформаційної безпеки відіграють важливу роль у забезпеченні захисту ІТ-систем;
- аудит і моніторинг (регулярні перевірки безпеки, моніторинг ІТ-систем для виявлення аномалій);
- фізична безпека (організація захисту фізичного доступу до серверних приміщень, обладнання та інфраструктури).

Одним із критичних для забезпечення кібербезпеки та ефективної роботи ІТ-систем чинників, який дає можливість суттєво підвищити рівень захищеності ІТ-систем і належить до елементів організаційної складової, має бути налагоджена взаємодія між підрозділами ІТ та інформаційної і кібербезпеки. Ключовими аспектами цієї взаємодії є:

- аналіз загроз і ризиків. Головним завданням спеціалістів підрозділу інформаційної та кібербезпеки є виявлення й оцінювання кіберзагроз для організації. Підрозділи інформаційної та кібербезпеки мають активно співпрацювати з підрозділами ІТ для аналізу можливих ризиків і вразливостей ІТ-систем та брати активну участь у розбудові та модернізації ІТ-систем для того, щоб зробити їх більш захищеними;

• впровадження технічних заходів безпеки. Підрозділ інформаційної та кібербезпеки сприяє впровадженню технічних рішень для захисту від загроз, які мають бути інтегровані в ІТ-інфраструктуру;

• розроблення та впровадження політик безпеки. Відповідальність підрозділу інформаційної та кібербезпеки за встановлення стандартів, розроблення процедур та вибір технологій, які допомагають захищати ІТ-системи. Важливо, щоб ці політики безпеки були відомі й виконувалися підрозділом ІТ;

• моніторинг та виявлення інцидентів (підрозділ інформаційної та кібербезпеки моніторить заходи безпеки та реагує на можливі кіберінциденти. Співпраця з підрозділом ІТ дає можливість ефективно виявляти та реагувати на аномалії в роботі ІТ-систем);

• реакція на кіберінциденти. Підрозділи ІТ та інформаційної і кібербезпеки мають працювати разом, щоб виявити причини, взяти на контроль ситуацію та запобігти подібним кіберінцидентам у майбутньому.

Отже, скоординована взаємодія підрозділів ІТ та інформаційної і кібербезпеки є важливим чинником у забезпеченні ефективного кіберзахисту.

Ще одним організаційним заходом, що може суттєво поліпшити захист ІТ-систем, є безпекова обізнаність (Security Awareness) її користувачів, співробітників підрозділів ІТ, інформаційної і кібербезпеки та керівництва. Проведення навчань та тренінгів із питань кібербезпеки допомагає збільшити уважність користувачів до потенційних загроз. Регулярні оновлення інструкцій та політик інформаційної і кібербезпеки відіграють таку саму важливу роль у забезпеченні захисту ІТ-систем, як і процес управління оновленнями (patch management) ПЗ.

Окремо треба зауважити, що навчання та тренінги треба проводити не лише для рядових користувачів, а й для технічних спеціалістів, які обслуговують ІТ-системи, та керівництва.

Тренінги для технічних користувачів мають складатися з таких напрямів:

• підрозділ ІТ як ціль атаки зловмисників (навчання, спрямоване на те, щоб показати, як зловмисники можуть полювати на сам підрозділ ІТ, зокрема внутрішні загрози та атаки, спрямовані на персонал ІТ. Усвідомлення правил адміністрування критично важливих ІТ-систем для функціонування організації, а також робота з конфіденційною інформацією щодо доступів та налаштування);

• небезпека, фішинг та соціальна інженерія. Тренінг щодо виявлення та уникнення фішингових атак, а також розпізнавання методів

соціальної інженерії, які на сьогодні існують. Незважаючи на сучасні методи протидії, цільовий фішинг досить часто досягає мети, оскільки користувач є найслабшою ланкою ІТ-систем з позиції інформаційної та кібербезпеки;

- огляд сучасних трендів кіберзагроз, які можуть стосуватися як ІТ-систем, так і безпосередньо підрозділу ІТ. Важливо розуміти сучасні методи атак та розвивати стратегії реагування. Акцент на основних принципах безпеки, таких як принцип найменшого доступу, шифрування, визначення безпеки ПЗ та інші;
- створення ІТ-спеціалістами важких та унікальних паролів там, де можливо використовувати мультифакторну аутентифікацію, дотримуватися кращих практик управління паролями;
- роз'яснення важливості вчасного оновлення ПЗ та систем для запобігання використанню вразливостей зловмисниками;
- безпека використання мобільних пристроїв та впровадження заходів для захисту конфіденційної інформації на них.

Security Awareness для керівників має важливе значення для забезпечення ефективної кібербезпеки в організації. Керівництво має бути сповіщене про загрози та брати активну участь у впровадженні стратегій кібербезпеки. Ось деякі аспекти Security Awareness для керівників:

- розуміння керівником кіберзагроз. Сучасні кіберзагрози та їхні можливі впливи на роботу організації;
- стратегії керівництва. Наголошення на важливості активної ролі керівництва у створенні стратегії кібербезпеки та впровадження відповідних політик безпеки;
- культура безпеки. Заохочення керівників до створення культури кібербезпеки в організації, де безпека інформації є важливою частиною корпоративного середовища;
- важливість лідерства. Пояснення, як лідерство впливає на ставлення персоналу до кібербезпеки та чому лідерам варто бути прикладом у дотриманні правил кібербезпеки;
- фінансові видатки на кібербезпеку. Розуміння того, як фінансові видатки на кібербезпеку можуть забезпечити довгостроковий захист організації;
- управління ризиками. Навчання керівників ефективно управляти ризиками та приймати стратегічні рішення для забезпечення кібербезпеки;
- відповідальність за дані. Розуміння відповідальності керівництва за захист конфіденційної інформації, даних співробітників та клієнтів;

• захист важливих елементів ІТ-систем. Усвідомлення важливості захисту критичної ІТ-інфраструктури та ІТ-систем, що визначаються як першочергові для продовження роботи організації;

• стратегії взаємодії з ІТ-підрозділом та інформаційної і кібербезпеки. Виявлення стратегій ефективної взаємодії та комунікації між керівництвом і підрозділами ІТ та інформаційної і кібербезпеки.

У наш час, коли кіберзагрози стають дедалі більш удосконаленими та розповсюдженими, Security Awareness стає критичним компонентом забезпечення ефективної кібербезпеки організації. Зростання кількості атак, високий рівень маскування кіберзагроз та умови роботи, що постійно змінюються, створюють необхідність для постійного вдосконалення знань та навичок персоналу.

Security Awareness не обмежується лише отриманням навичок розпізнавання фішингових листів чи використанням складних паролів. Він містить у собі розуміння комплексної природи кібербезпеки, важливості лідерства у створенні культури інформаційної та кібербезпеки і глибокої уваги до стратегічних рішень на рівні керівництва.

Отже, Security Awareness є важливою ланкою в ланцюжку захисту ІТ-систем, яка визначає успіх або невдачу в захисті інформації та ІТ-систем. Розуміння ризиків, виявлення загроз та усвідомлення відповідальності кожного працівника є ключем до створення культури інформаційної та кібербезпеки, яка стане опорою для відповіді на нинішні та майбутні кіберзагрози.

Таким чином, поєднання організаційної та технічної складових разом створює комплексний підхід до захисту ІТ-систем від різноманітних кіберзагроз. Ефективний захист ІТ-систем будь-якої організації потребує такого комплексного підходу та постійного вдосконалення. Лише узгоджена діяльність персоналу, своєчасні заходи безпеки та використання новітніх технологій можуть підвищити рівень захисту ІТ-систем від сучасних кіберзагроз.

4.3. Організація безпеки корпоративних баз даних

В епоху інформатизації та діджиталізації захист інформації – одне із важливих завдань, а цифрові дані – це критичний актив сучасних організацій. Щодня вони по всьому світу збирають та генерують велику кількість даних. У 2020 році об'єм створених та спожитих даних у світі був 64 ZBytes (зеттабайт), що становить 64 000 000 000 000 GB (64 трільярди GB) [23]. У 2021 році прогнозують зростання до 79 ZBytes, а у

2025-му прогнозується 181 ZBytes, тобто втричі більше, ніж у 2020 році (рис. 4.4). Сюди відносяться насамперед медіа-контент, big-data та корпоративні дані.

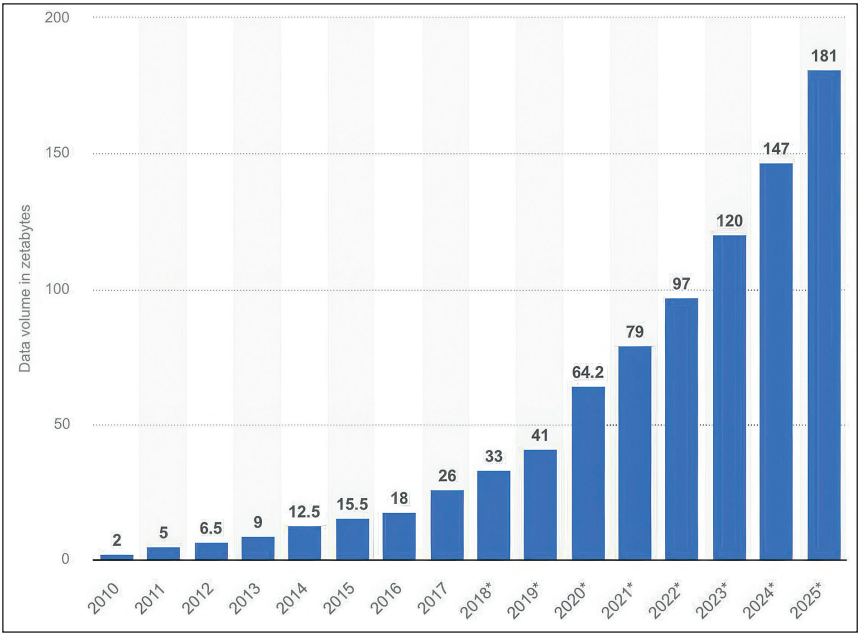

Рис. 4.4. Об'єми даних у глобальній мережі

Таке динамічне зростання об'єму даних формує нові завдання для організацій – їх зберігання та захист [24, 25]. Проте не завжди організації усвідомлюють важливість захисту власних даних.

4.3.1. Особливості використання корпоративних БД

У доцифрову епоху носіями інформації були паперові носії, що зберігалися в архівах. Тепер інформація прийняла цифрову форму та зберігається в автоматизованих цифрових БД. Серед них найбільш відомими є Oracle, MS SQL, MySQL, PostgreSQL, MongoDB та інші.

Використання автоматизованих БД дає можливість обробляти великі масиви даних, які були важкодоступними для обробки раніше. Організація в короткий термін може підготувати та опрацювати дані за тривалий період. Без використання БД така аналітика потребує значних

трудозатрат. Використання БД значно підвищує ефективність організації та забезпечує цілий пласт даних для подальшого аналізу та обробки.

Без використання автоматизованих БД не обходиться жодна IT-система обліку та управління організацією. Як наслідок БД посіли ключове місце у функціональних процесах організацій будь-якого масштабу.

4.3.2. Захист корпоративних БД

Важливим для економічної безпеки організації є захист корпоративних БД та інформації в них [26]. Захист інформації – це основне завдання процесу управління БД, який в англомовних джерелах називають database security. Захист БД містить такі компоненти (рис. 4.5):

1) фізичний захист БД;
2) захист продуктивності БД та їхній моніторинг;
3) захист даних у БД від знищення чи пошкодження;
4) контроль доступу;
5) облік нових БД, які з'являються в інфраструктурі.

У першу чергу, захист БД складається з фізичного захисту. Фізичний доступ до БД має бути обмеженим та доступним лише для авторизованого персоналу. Із розвитком хмарних технологій цей компонент інформаційної та кібербезпеки втратив свою актуальність, адже питанням фізичного доступу до обладнання, де зберігається інформація, займається постачальник хмарних сервісів. Утім, існує багато інших внутрішніх та зовнішніх загроз, основні з яких ми розглянемо далі.

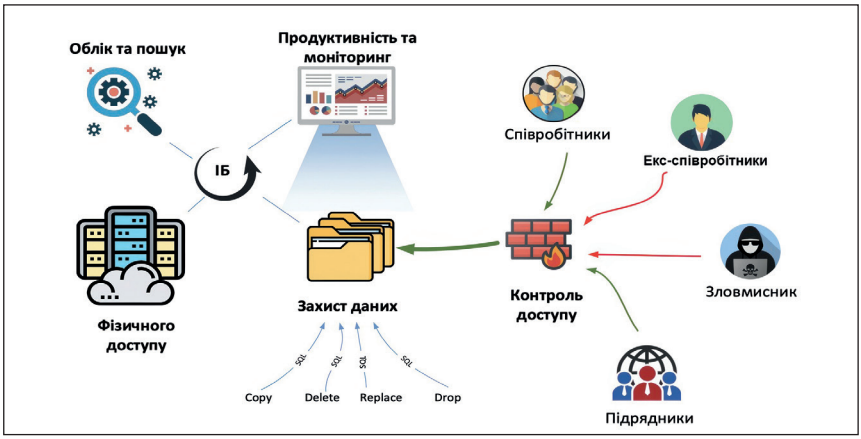

Рис. 4.5. Компоненти інформаційної безпеки БД

Надмірні права доступу. До БД мають доступ користувачі різних типів та рівнів доступу. Серед них:

- *внутрішні користувачі* – працівники, які мають доступ до БД напряму або через сторонні додатки;
- *системні адміністратори* – як правило, мають повні права доступу, а кількість адміністраторів може сягати десятків людей, тому виникає проблема контролю дій адміністраторів, використання паролів доступу, видачі та видалення прав доступу адміністраторам;
- *підрядники та партнери,* серед яких аутсорсери, розробники ПЗ, замовники (і подібні), яким доступ до БД надається для розроблення та тестування нового ПЗ, оформлення замовлень дочірніми організаціями, самообслуговування on-line чи технічного супроводу БД;
- *Machine-to-Machine (M2M) комунікації* – комунікація між технологічними системами. Це впровадження мобільних додатків, on-line-сервісів, взаємна інтеграція управлінських систем та інше. Характерною особливістю є використання API (Application Programming Interface). Більшість корпоративних даних обробляється із застосуванням M2M комунікацій (рис. 4.6).

Користувачі можуть зловживати наданим доступом до БД у таких напрямках:

- зловживання та використання надмірних прав доступу;
- зловживання об'єктивно-необхідними правами доступу;
- зловживання правами, які не використовуються.

Рис. 4.6. Комунікативні моделі людина-людина, людина-машина, машина-машина

Слабо контрольований процес видачі прав доступу до БД, як правило, формує надмірні права доступу, що завжди створює надлишковий ризик для інформаційної безпеки. Згідно зі статистикою, 80 % атак корпоративних БД виконуються працівниками або екс-працівниками.

До заходів безпеки відносять, по суті, запровадження процесу видачі та обліку виданих доступів, видача мінімально необхідних прав доступу та впровадження механізму контролю та блокування виданих доступів.

SQL Injections. Це вид атаки, при якому зловмисний SQL-код вбудовується у вебдодатки або вставляється зловмисником у текстові поля-форми на вебсайті (для заповнення прізвища, ім'я по батькові, номеру телефону, e-mail, тощо) [27].

Без відповідного захисту такий SQL-код може бути переданий від frontend (вебсайт, з яким працює користувач) до backend (внутрішня «сторона» вебсайту) та виконаним. Кіберзлочинець може отримати необмежений доступ до бази та виконувати SQL-команди безпосередньо в БД, наприклад, видалити чи скопіювати базу.

Виокремлюють два види атак:

- SQL injection атаки, спрямовані на традиційні БД;
- NoSQL (Not Only SQL) injection атаки, спрямовані на big data БД.

Як протидію визначають:

- використання Stored Procedure та API замість прямих SQL-команд [28];
- впровадження MVC (Model-View-Controller) архітектури [29];
- впровадження фаєрволу БД Imperva Database Security [30].

Низький рівень деталізації подій БД. Насамперед це важливо для банківської та фармацевтичної галузі, оскільки низький рівень відстеження подій у БД становить ризик невідповідності вимогам національних та міжнародних регуляторів стосовно обробки та зберігання конфіденційних даних. Усі транзакції БД повинні фіксуватися в автоматичному режимі з обов'язковим використанням сторонніх автоматизованих систем обстеження БД. Невиконання цих вимог формує значні ризики для БД на різних рівнях.

Способом зниження ризику в даному випадку є використання сторонніх автоматизованих систем аудиту БД (Audit Trail). Використання Imperva Database Security (Imperva DBS) є найкращим технологічним рішенням галузі.

Витік через резервні копії. Хорошою практикою є впровадження процесу регулярного резервування БД. Не менш важливим є впровадження механізму перевірки цілісності резервних копій та можливості відновлення бази з резервної копії.

Важливо також забезпечити захист резервних копій БД. Як правило, резервні копії, навіть із найбільш критичними даними, залишаються незахищеними від викрадення, знищення чи внесення змін. Незахищеність резервних копій формує високий ризик інформаційної безпеки організації.

Методи протидії:

- шифрування і бази, і резервних копій. Зберігання інформації в зашифрованому вигляді дозволяє забезпечити захист як продуктивної бази, так і її резервні копії. Imperva DBS – найкращий спосіб вирішити це завдання;
- відстежувати та регламентувати доступ до БД та її резервних копій.

Вразливості та налаштування. Часто БД повністю незахищена в результаті некоректного налаштування. Більшість БД мають власні системні облікові записи та конфігураційні параметри за замовчуванням. Крім того, розроблення програмного коду завжди супроводжується програмними дефектами. Для їхнього усунення компанії-виробники ПЗ випускають оновлення, патчі, інструкції з безпечного використання. Програмні дефекти формують вразливості ПЗ.

Зловмисники, як правило, є досить кваліфікованими для того, щоб знати, які вразливості вбудовані в ту чи іншу БД та які налаштування системи можна використати для несанкціонованого доступу.

Методи протидії:

- видалення облікових записів, які створені за замовчуванням;
- підвищення кваліфікації IT-персоналу;
- використання Imperva DBS для захисту БД від використання вразливостей ПЗ, виявлення використання підозрілих облікових записів та інше.

Denial of Service. Досить «старий», але ефективний вид атаки, який сповільнює роботу БД або виводить її з ладу, не дає можливості виконувати продуктивну роботу [31].

У складних випадках для зупинення DDoS-атаки компанії вдаються до відключення БД від мережі Інтернет. Це дозволить відновити роботу бази, проте включення інтернет-каналів знову активує DDoS-активність, що, у свою чергу, знову виводить базу з робочого стану. Хоча

DDoS-атака не має на меті викрадення чи пошкодження даних, проте може дорого обійтися підприємству, адже неможливість роботи з даними робить БД некорисною.

Методи протидії:

- використання Intrusion Detection System [32];
- постійний моніторинг активності БД, вивчення її вразливостей та блокування можливості їх використання;
- очищення трафіку за допомогою хмарних сервісів типу Imperva Cloud WAF (Web Application Firewall) [33].

Отже, найбільш дієвим засобом захисту БД є впровадження Imperva DBS та Imperva WAF – спеціалізованих програмно-апаратних комплексів, розроблених для захисту БД, захисту вебдодатків, очищення нелегітимного трафіку, захисту від використання вразливостей. Застосування Imperva DBS допоможе вирішити всі ключові завдання захисту БД і забезпечить повну видимість та контроль використання БД в інфраструктурі організації.

4.4. Тестування на проникнення як засіб підвищення рівня кібербезпеки інформаційних систем

4.4.1. Історія виникнення тестування на проникнення

Історія тестування на проникнення практично дорівнює історії IT-галузі. Ще у 1960-х рр., з появою перших великих обчислювальних мереж, таких як ARPANET, почали виникати і перші загрози безпеці, та під час роботи урядових організацій США, таких як RAND Corporation, зародилась ідея тестів на проникнення. 1980-ті рр., коли розвиток мережевих технологій призвів до поширення хакерських атак, як контрзахід з'явилася концепція «білих хакерів», які використовували свої навички для підвищення безпеки ІС. Це заклало основу для офіційного тестування ІС на проникнення [34]. 2000-ті рр. було ознаменовано формалізацією методологій: появою таких стандартів, як OSSTMM (Open-Source Security Testing Methodology Manual), NIST SP 800-115 (National Institute of Standards and Technology Special Publication) та OWASP (Open Web Application Security Project). Завдяки цьому тести на проникнення стали більш структурованими, а організації почали проводити їх на регулярній основі для забезпечення безпеки своїх ІС. 2010-ті рр. було ознаменовано появою різноманітних автоматизованих систем для тестування на проникнення, які можна використовувати онлайн, а також подальшим

поширенням цієї послуги, оскільки урядові організації по всьому світу почали вимагати проведення регулярних тестів на проникнення для забезпечення кібербезпеки критичної, державної та комерційної інфраструктури [35]. Тому завдання щодо підвищення рівня кіберзахисту ІС за рахунок застосування тестів на проникнення є дуже актуальним.

4.4.2. Основні класифікації тестів на проникнення

Тести на проникнення (англ. penetration tests) – це процеси, спрямовані на виявлення слабких місць в ІС, додатках або мережах шляхом симуляції реальних атак. Оцінювання захищеності комп'ютерної системи чи мережі відбувається шляхом часткового моделювання дій зовнішніх зловмисників із проникнення в неї (які не мають авторизованих засобів доступу до ІС) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу) [36]. Основою цього процесу стає активний аналіз ІС із виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних або технічних контрзаходах [37]. Зазначимо, що такий аналіз проводиться з позиції потенційного нападника і має включати активне використання вразливостей ІС, принаймні в частині тестування, що виконується експертом.

Зазвичай у ході тесту на проникнення виявляється певний набір вразливостей в ІС, яку було протестовано. Зібрана інформація оформлюється в стандартизований звіт, який представляють власнику системи. Важливою частиною такого звіту є аналіз, що поєднує цю інформацію з детальною оцінкою потенційного впливу на організацію та окреслює межі технічних і процедурних контрзаходів для зменшення ризиків.

Головною перевагою тестів на проникнення є рання ідентифікація ризиків: вони допомагають визначити слабкі місця до того, як їх використають зловмисники. Також регулярне тестування дозволяє організаціям покращити свою репутацію, бо таким чином вони демонструють свою відповідальність у питаннях кібербезпеки і кіберзахисту. У цілому тестування на проникнення все більше стають обов'язковими в різних регіонах та галузях економіки, завдяки тому, що допомагають продемонструвати відповідність вимогам таких стандартів, як ISO27001, SOC 2 (System and Organization Controls), PCI DSS (Payment Card Industry Data Security Standard) та інших.

4.4.3. За типом доступу до інформації

Існує багато різновидів тестів на проникнення. Найбільш поширеними є ті, що класифікуються за типом доступу до інформації, яка надається тестерам, та за основним об'єктом тестування.

Основні різновиди тестів на проникнення за типом доступу – це «чорна скринька» (англ. black box), «сіра скринька» (англ. gray box) та «біла скринька» (англ. white box). Тестування на проникнення типу black box відбувається тоді, коли тестери не мають жодної інформації про систему або мережу, яку вони тестують. Їхнє завдання – симулювати атаку з точки зору зовнішнього зловмисника, щоб виявити слабкості, доступні без внутрішньої інформації. Перевагами такого підходу є реалістичність та симуляція реальних зовнішніх атак. З іншого боку, потенційно це може призвести до пропущення вразливостей, які можуть бути виявлені при більш глибокому аналізі, оскільки тестери не завжди можуть ідентифікувати всі вразливості з таким підходом. У цьому варіанти тестування на проникнення багато залежить від знань тестера [38].

Тестування на проникнення типу grey box відбувається тоді, коли тестерам надають частковий доступ до внутрішньої інформації (документація, обмежені дані про архітектуру), що дозволяє ефективніше оцінити вразливості. Це імітує сценарій симуляції атаки інсайдера з обмеженим доступом; також добре підходить для тестування окремих компонентів системи. Такий підхід є певним компромісом між реалістичністю та глибиною аналізу, проте він вимагає більше часу, ніж black box, але менше, ніж із white box. Як і у випадку з black box, такий підхід потенційно може призвести до пропуску вразливостей через обмежений доступ, що може бути викликано складнощами визначення обсягу інформації, яка надається тестерам [39].

У випадку з white box підходом тестери мають повний доступ до інформації про систему, включаючи архітектуру, код, мережеві топології та ін. Цей підхід використовують з метою здійснити найглибший аналіз безпеки, наприклад, під час аналізу коду додатків або перевірки комплексної архітектури системи. Незважаючи на безумовні переваги такого підходу, він не завжди здатний врахувати реалістичні варіанти атаки зовнішнього зловмисника та вимагає значних витрат часу і ресурсів [40].

Кожен із вищеназваних підходів до тестування має свої переваги та недоліки. Вибір підходу залежить від цілей тестування: якщо для перевірки зовнішньої безпеки доцільно використовувати black box, то для

аналізу внутрішніх компонентів чи специфічних вразливостей підійде grey box. Для детального аудиту безпеки системи краще підходить white box підхід.

4.4.4. За типом об'єкта доступу

Розглянемо основні різновиди тестів на проникнення за об'єктом доступу.

Тестування вебзастосунків (Web Application Pentesting):

- тестування мобільних застосунків (Mobile Application Pentesting),
- тестування мереж (Network Pentesting),
- тестування бездротових мереж (Wireless Network Pentesting),
- тестування соціальної інженерії (Social Engineering Pentesting)
- фізичне тестування на проникнення (Physical Pentesting).

Варто зазначити, що всі вищезгадані типи тестування на проникнення потребують спеціальних знань та навичок. Розглянемо ці типи детальніше.

Тестування вебдодатків (Web Application Pentesting). Цей тип тестування на проникнення спрямований на виявлення вразливостей у вебдодатках. Це досить складний процес, оскільки він охоплює фронтенд, базу даних, бекенд та інші складові вебдодатку, щоб ідентифікувати вразливості в коді, конфігурації або архітектурі вебдодатків. У межах тестування перевіряються всі кінцеві точки взаємодії застосунку з користувачем. Деякі перевірки, які можуть бути частиною такого оцінювання безпеки, включають: використання відкритих джерел (OSINT); визначення серверів, IP-адрес, субдоменів; аналіз HTTP-запитів (Hypertext Transfer Protocol) та заголовків; атаки типу Cross-Site Scripting, клікджекінг, викрадення форм, HTML-ін'єкції, відкриті перенаправлення та багато інших [41].

Тестування мобільних додатків (Mobile Application Pentesting). Цей тип тестування на проникнення стає надзвичайно популярним, оскільки все більше бізнесів та державних сервісів використовують мобільні додатки. Тестування мобільних додатків включає такі перевірки, як: отримання інформації про додаток, сервери та API; аналіз архітектури додатка (мобільна частина, бекенд, API); збирання даних про залежності та бібліотеки; перевірка поведінки додатка під час виконання; моніторинг трафіку між клієнтом та сервером; аналіз уразливостей API; перевірка механізмів аутентифікації та авторизації тощо. Симуляція атак для підтвердження знайдених вразливостей у мобільному додатку може

підтвердити такі вразливості, як небезпечне зберігання даних, недостатнє шифрування чи механізми аутентифікації даних, помилки валідації введення, відкриті API тощо [42].

Тестування мереж (Network Pentesting). Це один із найпоширеніших типів тестування на проникнення, який спрямований на виявлення вразливостей та слабких місць у мережевій IT-інфраструктурі. Сюди входять не лише MME (firewalls), комутатори та маршрутизатори, але й сервери, сховища даних, робочі станції, принтери тощо. Цей тип тестування допомагає оцінити рівень готовності до атак, таких як обхід MME, атаки на маршрутизатори, проксі-сервери, бази даних тощо. Такі тестування передбачають ідентифікацію мережевих сегментів, зокрема LAN (Local Area Network), WAN (Wide Area Network), VPN (Virtual Private Network); визначення обладнання; встановлення рівня тестування – зовнішній (External) або внутрішній (Internal); аналіз відкритих портів і служб; визначення потенційних вразливостей; аналіз неправильно налаштованих мережевих служб; ідентифікацію застарілих протоколів (наприклад, SMBv1 (Server Message Block), FTP (File Transfer Protocol)); атаки на слабкі паролі; експлуатацію вразливих служб (наприклад, RDP (Remote Desktop Protocol), SSH (Secure Shell)); оцінку глибини компрометації та пошук шляхів для горизонтального або вертикального переміщення в мережі [43].

Тестування бездротових мереж (Wireless Network Pentesting). Це специфічний тип тестування мереж, який зосереджується на з'єднаннях між бездротовими пристроями та домашніми чи офісними Wi-Fi-мережами. Особливість бездротового пентесту полягає в тому, що він виконується на місці, оскільки потрібно знаходитися в зоні дії сигналу. Проте певні пристрої можуть підключатися до бездротової мережі, що дозволяє віддаленому тестувальнику проводити перевірки. Бездротові мережі необхідно тестувати, оскільки вони є одним із найпоширеніших джерел витоку даних через їх відносно менш контрольований характер використання.

Тестування соціальної інженерії (Social Engineering Pentesting). Цей тип тестування відрізняється від інших, оскільки більше покладається на соціальні, комунікаційні та, певною мірою, дизайнерські навички, а не суто технічні. Під час соціальної інженерії зловмисник намагається змусити жертву розкрити чутливу інформацію, наприклад, облікові дані. Існує широкий спектр технік соціальної інженерії, таких як фішинг, вішинг, смішинг, атаки видавання і багато інших.

Незважаючи на здавалося б менш агресивний характер соціальної інженерії, це небезпечна ілюзія. Вражаючі 98 % усіх кібератак зараз використовують елементи соціальної інженерії [44]. Такі атаки занадто часто виявляються успішними, оскільки людський фактор залишається найслабшою ланкою у складній системі кібербезпеки. Тестування соціальної інженерії, поєднане з навчанням підвищення обізнаності про кібербезпеку, стало основою сучасної кібербезпеки будь-якої організації.

Фізичне тестування на проникнення (Physical Penetesting). Цей тип тестування на проникнення теж є специфічним, однак стоїть трохи осторонь інших типів, оскільки обов'язково передбачає спроби обійти фізичні бар'єри, такі як замки, камери, паркани, різні датчики тощо, що захищають певну інфраструктуру чи системи. Це – моделювання дій потенційного зловмисника, який намагається отримати доступ до об'єктів, приміщень або критичних фізичних ресурсів. Цей тип тестування дозволяє виявити слабкі місця у фізичній безпеці, таких як системи контролю доступу, відеоспостереження, або поведінкові аспекти співробітників [45]. У типовому фізичному тестуванні на проникнення відбувається визначення ключових об'єктів, таких як серверні кімнати, склади, офіси тощо; проходить оцінювання систем захисту: сигналізації, охорони, замків, камер; узгоджуються дозволені та заборонені методи тестування, та після цього починається сам процес, що передбачає спостереження, аналіз та спроби фізичного проникнення на об'єкт.

Отже, зазначимо, що обидві вищезгадані класифікації – за типом доступу до інформації та за об'єктом тестування – можна та треба використовувати в комбінації, бо, за деякими винятками, кожен із тестів на проникнення буде відповідати одному з типів з обох класифікацій.

Таким чином, тестування на проникнення є одним з основних типів оцінювання рівня кібербезпеки ІС та засобом його підвищення. Сьогодні розвиток напрямку тестування на проникнення поєднує тренди на подальшу автоматизацію, використання хмарних інструментів, ШІ в аналізі вразливостей, збільшення ролі тестів, що використовують соціальну інженерію [46]. Тестування на проникнення продовжать своє подальше поширення й розвиток методологічної та інструментальної компонент.

4.5. Керування вразливостями в IT-системах

4.5.1. Виникнення та розвиток

Поява та розвиток процесу керування вразливостями в IT-системах нерозривно пов'язані із самою історію IT. З 1970-х рр. та аж до кінця 1990-х питання безпеки в персональних і корпоративних мережах вирішувалися здебільшого ситуативно та хаотично: окремі адміністратори патчили системи, виправлення розповсюджувалися вручну або через вузькі корпоративні канали. Інструменти автоматизованого сканування та централізованого управління були експериментальними або дорогими, а стандарти, по суті, відсутні.

Епохальною подією в цій галузі стала поява CVE (Common Vulnerabilities and Exposures) у 1999 році [47]. Це – загальнодоступний реєстр ідентифікованих вразливостей, що стало фундаментом для уніфікації назв, обміну інформацією й інструментального екосистемного зростання (сканери, бази даних, експлойт-фідери). Завдяки кодифікації вразливостей CVE надала «єдину мову», необхідну для кооперації в рамках загального процесу керування вразливостями (Vulnerability Management, VM).

Поява реєстру CVE відкрила шлях для бурхливого розвитку цього напрямку IT-послуг, оскільки з'явилась організаційна можливість забезпечити автоматизоване виявлення вразливостей для широкого кола державних та приватних організацій. На зламі тисячоліть почали з'являтися різноманітні комерційні продукти, зокрема такі, як Nessus, який наразі став де-факто галузевим стандартом, і сервіс-моделі, а також формуватися перші практики централізованого управління базами вразливостей в окремих організаціях [48].

Наступним суттєвим кроком вперед стало розроблення CVSS (Common Vulnerability Scoring System), або системи порівняння вразливостей на основі загальних основі метрик впливу та ймовірності експлуатації. Паралельно такі агрегатори даних щодо вразливостей, як NVD (National Vulnerability Database), стали ключовими репозитаріями, що забезпечували метадані для VM-інструментів, які можуть зчитуватися машинами. Ці здобутки радикально підвищили масштаби й можливості автоматизації для інструментів VM [49].

У минулому десятиріччі, у зв'язку зі стрімким розвитком цифрової інфраструктури веб- та мобільних додатків, на фоні з розвитком хмарних моделей організації IT-систем взагалі та особливо процесів

розроблення ПЗ, зокрема – контейнеризації, на перший план вийшла інтеграція практики VM у процеси розроблення. Сканування коду під час розроблення та релізів програмних продуктів призвели до подальшого розвитку методології керування вразливостями, яка тепер вміщувала не лише базове сканування та ранжування на основі CVEE, але й пріоритизацію на основі експлуатаційних спостережень. На новий рівень вийшла також автоматизація VM: нормальною практикою стало автоматичне створення завдань для IT-фахівців за результатами чергового автоматичного сканування тієї чи іншої IT-системи.

Починаючи із 20-х рр. акцент у розвитку практик VM змістився на подальше підвищення практичності оцінювання вразливостей. Через стрімке зростання масштабу та складності IT-ландшафту звичайної системи CVE стало недостатньо для ефективного керування вразливостями, та у відповідь на це почали виникати так звані ймовірнісні моделі (probabilistic models), наприклад KEV (Known Exploited Vulnerabilities), яка дозволила реалізувати на практиці автоматизацію оцінювання знайдених вразливостей щодо ймовірності їхньої експлуатації в реальних сценаріях, тобто створення переліків вразливостей на першочергове виправлення [50].

4.5.2. Керування вразливостями та його складові

Керування вразливостями – це організаційно-технічний процес і набір практик для виявлення, оцінки, пріоритизації, усунення (або пом'якшення) і валідації вразливостей у програмному та апаратному забезпеченні в IT-системах та системах промислової автоматизації, які використовують державні та комерційні установи. Під вразливістю розуміється помилка або слабкість у дизайні, реалізації чи управлінні інформаційної системи, яку може експлуатувати зловмисник і яка може призвести до порушення конфіденційності, цілісності або доступності системи [51].

У загальному процесі VM ключову роль відіграє сканування, як мережеве, так і кінцевих точок; збирання контексту щодо IT-середовища; математичні / статистичні моделі пріоритизації знахідок; операційні процеси реагування, такі як планування патчів, або відкат за потреби. Повторюваний цикл VM можна розглядати як безперервний ланцюжок (рис. 4.7).

Рис. 4.7. Повторюваний цикл VM

Цей підхід відповідає сучасним настановам із патч-менеджменту і технічних оцінок [52, 53].

Багато нефахівців, а подекуди навіть деякі фахівці часто утотожнюють процеси керування вразливостями та сканування на вразливості, але це не є коректним. Якщо перше – це загальний процес, то сканування – лише техніка з першої стадії «виявлення». Сканер сам по собі видає сигнали (alerts), які треба нормалізувати, верифікувати та прив'язати до контексту – інакше численні помилково-позитивні або неактуальні знахідки перевантажують операції і знижують ефективність. Сканування – необхідне, але недостатнє; VM – це система процесів, людей і даних, що перетворює результати сканерів на відтворювані управлінські рішення [54]. Таким чином, сканування є ядром процесу VM: воно забезпечує систематичний пошук відомих слабких місць у ПЗ, конфігураціях і мережевих сервісах. На практиці використовують три основні підходи:

- мережеве сканування (remote network-based);
- агентське сканування (host-based з агентами);
- аналіз прикладного рівня та вебдодатків (DAST – Dynamic Application Security Testing, SAST – Static Application Security Testing, IAST – Interactive Application Security Testing).

Результати сканування мають пройти верифікацію, фільтрацію та пріоритизацію. Без цього може виникнути парадокс, коли організація отримує десятки тисяч знахідок, з яких значна частина є неактуальною або помилковою. Це призводить до перевантаження інформацією (alert fatigue), втрати довіри до інструментів і зниження швидкості реагування [55].

4.5.3. Виклики процесу VM

Розриви покриття. Важливість та складність організації процесу VM у сьогоденних IT-середовищах важко переоцінити, перш за все, через постійно зростаючу складність та гетерогенність IT-систем, які в сучасних організаціях дедалі рідше є монолітними чи статичними. Натомість вони розвиваються як динамічні екосистеми, що включають локальні дата-центри, хмарні сервіси, гібридні архітектури, контейнеризовані мікросервіси, а також IoT (Internet of Things). Така гетерогенність створює серйозні виклики для процесу управління вразливостями IT-систем, оскільки вони стикаються з так званими розривами покриття (coverage gaps) – коли сканери вразливостей або процеси управління не виявляють, не враховують чи не встигають обробити частину потенційних точок ризику.

До основних факторів, які обумовлюють існування «розривів покриття», відносять такі:

1) різнорідність технологій: у складних IT-середовищах поєднуються застарілі системи (legacy), сучасні сервери, мобільні пристрої, віртуальні машини, контейнери та IoT. Багато вразливостей є специфічними для окремих платформ, і традиційні сканери не завжди мають необхідні плагіни чи сигнатури [56];

2) динаміка хмарних середовищ та контейнерів: широко вживані сьогодні контейнери та оркестратори (Docker, Kubernetes) створюють IT-середовища з високою швидкістю змін. Активи можуть існувати лічені хвилини, перш ніж зникнути або бути заміненими. Це ускладнює повноцінне покриття та вчасне виявлення вразливостей, які, утім, можуть бути використані зловмисниками [57];

3) «сліпі зони» в мережі: в умовах розповсюдження сегментації мережі та багаторівневої віртуалізації сканери можуть не бачити певних підмереж або закритих середовищ, особливо в хмарах чи середовищах з обмеженим доступом [58];

4) людський фактор і процесні прогалини: керування вразливостями передбачає інтеграцію технічних та організаційних процесів, але на практиці ці процеси навіть сьогодні постійно стикаються з неповними або неточними інвентаризаціями активів, відсутністю оновлених політик, а також із таким чинником, як перевантаження інформацією. У комплексі це постійно призводить до того, що навіть відомі вразливості залишаються невиправленими [59].

Наслідками цих факторів стає те, що в IT-керівництва організацій може з'являтися хибне відчуття безпеки, коли є впевненість, що покриття повне, хоча насправді критичні активи залишаються поза увагою. Також існує велика небезпека асиметричних ризиків, коли «розриви покриття» з'являються саме в найбільш динамічних зонах – хмарних середовищах, мобільних додатках, IoT, які одночасно є й найпривабливішими для атак. У комплексі все це призводить то системної вразливості, коли навіть один «невидимий» актив може стати точкою входу для атаки з ефектом доміно. З іншого боку, існують рішення для всіх цих проблем, зокрема:

- інвентаризація IT-активів у режимі реального часу;
- агентське та безагентське сканування в комбінації, що дозволяє покривати як постійні активи, так і швидкоплинні середовища;
- адаптивне управління ризиками, де пріоритети визначаються на основі контексту критичних активів, а не лише CVSS-рейтингу;

- використання людиноцентричних методів (психоедукація фахівців із кібербезпеки, управління когнітивним навантаженням, автоматизація первісного аналізу результатів сканувань).

Хибнопозитивні і хибнонегативні результати. Хибнопозитивні (False Positives, FP) результати сканування виникають, коли сканер повідомляє про вразливість там, де її немає. Серед найпоширеніших причин появи хибнопозитивних результатів: евристичний характер перевірок, коли результат сканування схожий на вразливу версію, але патч уже встановлено; обмежена видимість через блокування фаєрволом або нестандартні конфігурації ІТ-середовища; недостатня актуальність сигнатур. Знахідки типу FP підривають довіру до самого процесу керування вразливостями [60].

Хибнонегативні результати є ще більш небезпечними (False Negatives, FN), бо ІТ-персонал організації може бути впевненим, що її ІТ-системи є безпечними, хоча насправді вони знаходяться під ризиком. Серед основних причин виникнення FN:

- використання нових або 0-day вразливостей, відсутніх у базах CVE;
- наявність складних ІТ-середовищ, наприклад, із контейнерами або мікросервісами;
- просунуті обхідні техніки зловмисників, які змінюють сигнатури або структуру атак.

Основні підходи до зниження кількості FP/FN:

1. Комбіноване використання інструментів, насамперед сканерів, коли кілька з них дають різні покриття, й агрегація результатів знижує кількість FN.

2. Кореляція з іншими джерелами, такими як дані KEV/EPSS, БД відомих експлойтів вразливостей тощо. Це дозволяє відсіяти FP та підсвітити найбільш релевантні CVE.

3. Валідація знахідок через практичні тести, насамперед через тести на проникнення, які пропонують найвищу достовірність щодо знахідок, але вимагають суттєвих витрат.

4. Автоматизація контекстуалізації, коли використання різних технік та інструментів інвентаризації програмних та апаратних ІТ-активів дозволяє відфільтровувати нерелевантні CVE.

4.5.4. Прогнозування ймовірності експлуатації вразливості

Впровадження CVE було значним кроком вперед у керуванні вразливостями в IT-системах, але цього виявилося недостатньо. Практика багатьох років продемонструвала, що насправді експлуатується лише невелика частка CVE, через що підхід «патчити все критичне» виявився недостатньо ефективним. Це сталося тому, що насправді питання «які вразливості виправляти першими» виявилося одним із найкритичніших у процесі керування вразливостями. І протягом тривалого часу організації спиралися на систему CVSS як основний інструмент оцінки критичності вразливостей. Простий підхід «виправляємо все, що має CVSS ≥ 7.0» або «все критичне» здавався ефективним, але на практиці призводив до перевантаження фахівців, оскільки щороку виявляються десятки тисяч нових CVE. Поглиблений статистичний аналіз із метою вирішення цієї проблеми показав, що CVSS як ізольований показник не відображає реальної експлуатаційності вразливостей та контексту бізнес-ризиків. Хоча CVSS надає числове значення критичності на основі базових, часових і контекстних метрик, він не відображає динаміку загроз [61]. Це створювало перекіс: багато вразливостей із CVSS 9.0+ ніколи не експлуатувалися, тоді як експлойти «середніх» уразливостей активно використовувалися зловмисниками. Саме це привело до еволюції від «CVSS-порогів» до ризик-орієнтованої пріоритизації, що враховує ймовірність експлуатації, активність атак, контекст активу та потенційний вплив на функціонування організації.

Подальшим кроком стало створення EPSS (Exploit Prediction Scoring System) – відкритої моделі, що прогнозує ймовірність експлуатації вразливості на основі статистики CVE, експлойтів і поведінки атакувальників [62]. Це стало поворотним моментом, оскільки організації отримали змогу ранжувати не лише «наскільки небезпечна вразливість за CVSS», а й «наскільки ймовірно, що вона буде використана найближчим часом».

Завдяки цим змінам сучасна пріоритизація знахідок у процесі VM є ризик-орієнтованою та спирається на багатофакторні моделі. Серед факторів, що враховуються, основними є:

- експлуатаційність: чи існують публічні експлойти, чи зафіксовано активні атаки;
- властивості IT-активу: критичність для організації, чутливість даних, роль в архітектурі;
- динамічні фактори: наявність патчів, складність виправлення, можливість застосування компенсуючих контролів;

• прогнозованість: використання машинного навчання для прогнозування появи експлойтів або масштабності атак [63].

Такий підхід дає організаціям можливість приділити першочергову увагу не «всім CVSS ≥ 9.0», а тим уразливостям, які мають високу ймовірність експлуатації, стосуються критичних активів та вже потрапили до списків активно експлуатованих (наприклад, CISA KEV).

4.5.5. Сканери вразливостей як інструмент процесу VM

Сканери вразливостей стали базовим інструментом не лише VM, а й кібербезпеки взагалі ще з початку 2000-х років, коли з'явилися такі продукти, як Nessus, OpenVAS чи Qualys [64]. Вони дозволили автоматизувати виявлення відомих уразливостей у мережах, ОС та вебдодатках. Проте розвиток технологій, перехід до хмарних і контейнерних середовищ, а також зростання кількості вразливостей висвітлили низку обмежень, які сьогодні вважаються критичними:

1. *Хибнопозитивні та хибнонегативні результати*. Жоден сканер не забезпечує повної точності. Хибнопозитиви призводять до перевантаження аналітиків і зниження довіри до результатів, тоді як хибнонегативи створюють небезпечні «сліпі зони» [65].

2. *Залежність від сигнатур і баз CVE*. Більшість сканерів працює за принципом пошуку відомих патернів. Це означає, що нові чи zero-day вразливості залишаються поза увагою до моменту оновлення бази [66].

3. *Обмежене охоплення сучасних технологій*. Контейнеризовані середовища, мікросервіси, безсерверні функції (serverless) часто не мають достатнього рівня інтеграції зі сканерами. Це ускладнює повноцінний моніторинг у DevOps-середовищах

4. *Проблеми масштабування*. У великих організаціях із тисячами активів регулярні повні скани створюють значне навантаження на мережу, що може впливати на продуктивність IT-систем [67].

Відсутність контексту ризику. Сканери виявляють вразливості, але не враховують критичність активу, на якому знайдено проблему. Це знижує цінність результатів для прийняття рішень на рівні CISO (Chief Information Security Officer) [68].

Обмежений аналіз експлуатаційності. Хоча деякі сучасні рішення інтегрують дані EPSS чи threat intelligence, більшість класичних сканерів не прогнозують імовірність реальної експлуатації [69].

На сьогодні розроблено цілу низку способів щодо зменшення впливу цих обмежень:

1. *Поєднання агентських і безагентських методів*. Агентське сканування дозволяє отримувати точніші дані без перевантаження мережі, тоді як безагентське забезпечує ширше охоплення. Комбінація двох підходів зменшує прогалини.

2. *Інтеграція з контекстними системами*. Зв'язок сканерів із SIEM та системами управління IT-активами дозволяє враховувати бізнес-критичність уразливостей.

3. *DevSecOps-процеси*. Інтеграція сканування в CI/CD (Continuous Integration/Continuous Deliver) пайплайни та інфраструктуру як код дозволяє виявляти проблеми ще до етапу розгортання [70].

4. *Використання threat intelligence*. Додавання даних із CISA KEV, експлойт-баз і EPSS допомагає відсіяти «шум» та фокусуватися на реально небезпечних уразливостях [71].

5. *Людиноцентричні практики*. Автоматизація сортування знахідок, навчання аналітиків та зменшення інформаційного перевантаження підвищують ефективність роботи з результатами сканування.

Отже, сканери вразливостей залишаються необхідним, але не достатнім інструментом кіберзахисту. Вони добре працюють у виявленні відомих проблем, однак їхні обмеження вимагають доповнення іншими методами: контекстним аналізом ризиків, інтеграцією з DevSecOps-процесами, використанням прогнозних моделей та аналітики загроз. У майбутньому тенденція рухається до інтелектуального управління вразливостями, де сканери стають лише одним із модулів у ширшій екосистемі кіберзахисту.

4.6. Безпечне розроблення програмного забезпечення

Secure Software Development Life Cycle (SSDLC) – це підхід до розроблення ПЗ, який включає аспекти безпеки на всіх етапах життєвого циклу розроблення [72]. Мета SSDLC полягає в тому, щоби забезпечити створення ПЗ, стійкого до кібератак. Основні етапи SSDLC охоплюють: аналіз вимог, проєктування, розроблення, тестування, розгортання, технічну підтримку та обслуговування [73].

1.*Аналіз вимог.* Аналіз вимог до безпеки на етапі безпечного розроблення є фундаментальним для створення безпечного ПЗ. Цей етап передбачає ідентифікацію та документування всіх вимог безпеки, які має виконувати розроблюване ПЗ. Він починається до власне процесу розроблення і включає збирання вимог від зацікавлених сторін, таких як бізнес-аналітики, клієнти, кінцеві користувачі, а також експерти з безпеки. Аналіз вимог до безпеки передбачає такі кроки:

- визначення вимог – опрацювання та аналіз вимог до безпеки, які мають бути враховані в новому або оновленому ПЗ;
- оцінка ризиків – ідентифікація потенційних загроз та вразливостей, з якими може зіткнутися ПЗ;
- розроблення стратегії безпеки – створення плану заходів безпеки, що мають бути інтегровані в ПЗ;
- врахування регуляторних вимог – переконання, що ПЗ відповідає всім необхідним законодавчим та регуляторним вимогам.

Цей етап важливий, оскільки він допомагає встановити фундамент безпеки на самому початку життєвого циклу розроблення, що може значно зменшити ризики та вартість виправлення вразливостей у майбутньому. За допомогою аналізу вимог до безпеки команди розробників можуть визначити, які заходи безпеки потрібно вжити для захисту ПЗ від потенційних кібератак.

2. Проєктування. Проєктування як етап безпечного розроблення ПЗ відіграє ключову роль у впровадженні вимог безпеки в програмний продукт. Під час цього етапу команда розробників складає детальний план ПЗ, який повинен включати архітектуру системи, модулі, інтерфейси, а також визначає, як будуть реалізовані вимоги безпеки, встановлені на попередньому етапі аналізу вимог. Основні кроки проєктування в рамках SSDLC:

- розроблення архітектури – визначення структури системи, яка має підтримувати безпеку на всіх рівнях: від мережевих протоколів до додаткових шарів, таких як брандмауери та антивіруси;
- моделювання загроз – визначення потенційних загроз кожного компонента системи й розроблення моделі загроз, яка допомагає прогнозувати та запобігати можливим векторам атак;
- визначення контрзаходів – розроблення специфічних технічних рішень, що мають запобігати або пом'якшувати вплив виявлених загроз;
- проєктування бази даних – забезпечення цілісності, конфіденційності та доступності даних шляхом проєктування безпечних баз даних із належними рівнями доступу;
- розроблення політик безпеки – формування внутрішніх політик та процедур, які регулюють процеси розроблення та впровадження ПЗ;
- оцінка відповідності – переконання в тому, що проєкт відповідає всім регуляторним та галузевим стандартам безпеки.

У процесі проєктування важливо також здійснювати постійний зворотний зв'язок із зацікавленими сторонами, а також проводити регулярні огляди дизайну, щоб переконатися, що вимоги безпеки не просто включені до плану, а й ефективно інтегровані в саме ПЗ.

3.*Розроблення.* Етап розроблення в рамках безпечного життєвого циклу розроблення ПЗ включає безпосередньо створення програмного коду з використанням визначених архітектурних шаблонів та вимог до безпеки. На цьому етапі розробники імплементують функціональність програми, одночасно інтегруючи механізми безпеки, такі як аутентифікація, авторизація, шифрування даних, валідація введення та обробка помилок. Основні завдання під час розроблення:

- кодування – написання коду згідно з проєктними специфікаціями та вимогами до безпеки, використання стандартів безпечного кодування для запобігання вразливостям;
- перевірка коду – використання статичного аналізу коду та інших інструментів для раннього виявлення помилок та вразливостей;
- модульне тестування – тестування окремих частин програми (модулів) для перевірки їхньої функціональності та безпеки;
- інтеграційне тестування – перевірка взаємодії між різними модулями та компонентами системи, а також валідація інтеграції заходів безпеки;
- ревізія та оцінка коду – внутрішній та зовнішній аудит коду з боку експертів із безпеки для оцінки дотримання вимог безпеки;
- оптимізація – покращення продуктивності та ефективності коду, зниження його складності та видалення зайвого коду;
- документування – запис усіх процедур розроблення та інтегрованих заходів безпеки для подальшого використання та підтримки.

Цей етап SSDLC вимагає тісної співпраці між розробниками, тестувальниками та експертами з безпеки для забезпечення того, що ПЗ не лише виконує свої функціональні завдання, але й має високий рівень захисту від можливих загроз. Важливо пам'ятати, що заходи безпеки мають бути вбудовані в продукт із самого початку, а не додаватися після завершення розроблення.

4.*Тестування.* Тестування в контексті безпечного розроблення ПЗ є критично важливим етапом, який впливає на здатність продукту протистояти зовнішнім загрозам і вразливостям. Його основна мета – забезпечити, щоб усі аспекти безпеки були ретельно перевірені і щоб програмне забезпечення не містило відомих вразливостей, які можуть бути експлуатовані зловмисниками.

На відміну від звичайного тестування, яке зосереджене на перевірці функціональності та продуктивності ПЗ, до тестування в рамках SSDLC входять такі спеціалізовані види тестування, як:

- статичний аналіз коду (SAST) – автоматизована перевірка вихідного коду на предмет уразливостей без виконання коду;

- динамічний аналіз коду (DAST) – тестування запущеної програми на виявлення вразливостей, що можуть бути експлуатовані в реальному часі;
- тестування на проникнення – це симуляція атак зловмисників на ПЗ із метою виявлення незахищених точок в'їзду та інших потенційних слабкостей;
- тестування залежностей і компонентів – перевірка сторонніх бібліотек та модулів, які використовуються в програмному продукті, на наявність уразливостей;
- тестування конфігурації – переконання, що конфігурації системи та мережі встановлені безпечним чином;
- аудит коду – ручний огляд коду з метою виявлення потенційних уразливостей, які могли упустити автоматизовані інструменти.

Тестування безпеки має бути інтегроване в кожен етап SSDLC, починаючи з аналізу вимог і закінчуючи післявипускними оновленнями та підтримкою. Воно гарантує, що безпека є не просто додатком до продукту, а вбудована в його структуру із самого початку. Ключовою складовою ефективного тестування безпеки є освіта та тренінги для розробників та тестувальників, щоб вони могли розпізнавати і виправляти вразливості, а також використовувати найкращі практики безпеки під час написання та перевірки політик безпеки.

5.*Розгортання.* Розгортання ПЗ в SSDLC як завершальний етап безпечного розроблення є також критичним компонентом, що гарантує, що програмний продукт не лише відповідає вимогам безпеки, але й готовий до використання в реальних умовах. Цей етап містить кілька ключових дій, спрямованих на забезпечення того, щоб програмна система була готова до експлуатації:

Перевірка безпеки та відповідності. Перед розгортанням програмного забезпечення необхідно здійснити остаточну перевірку безпеки для виявлення будь-яких невирішених уразливостей чи проблем безпеки. Також важливо забезпечити відповідність усім необхідним стандартам та регуляціям безпеки.

Підготовка середовища. Розгортання вимагає підготовки середовища, де програмне забезпечення буде експлуатуватися. Сюди входить: налаштування серверів, БД, мережевих компонентів та інших залежностей.

Автоматизація розгортання. Використання інструментів для автоматизації розгортання може значно знизити ризики, пов'язані з людським фактором, та забезпечити більшу консистентність та надійність процесу.

Моніторинг та логування. Після розгортання важливо забезпечити належний моніторинг системи та логування подій, щоб бути в змозі швидко виявляти та реагувати на будь-які проблеми безпеки.

Оновлення та підтримка. Розгортання не є кінцевим етапом життєвого циклу програмного продукту. Важливо забезпечити регулярні оновлення та підтримку програмного забезпечення для виправлення вразливостей та покращення функціональності.

Розгортання ПЗ в контексті SSDLC вимагає інтеграції практик безпеки на кожному кроці процесу, починаючи від ініціального розроблення до остаточного розгортання. Це дозволяє забезпечити, що ПЗ не просто відповідає вимогам функціональності, але й мінімізує можливі ризики.

6. Технічна підтримка та обслуговування. Технічна підтримка та обслуговування ПЗ є важливими складовими безпечного розроблення ПЗ. Цей етап забезпечує неперервну підтримку і вдосконалення ПЗ після його розгортання та впровадження в експлуатацію. Основна мета полягає в забезпеченні стабільності, безпеки та актуальності програмного продукту протягом усього періоду його використання. Основні аспекти технічної підтримки та обслуговування в SSDLC:

Виявлення та усунення помилок. Навіть після ретельного тестування в ПЗ можуть виявлятися помилки. Технічна підтримка займається ідентифікацією, аналізом та усуненням цих помилок.

Оновлення безпеки. Це регулярне оновлення ПЗ для захисту від нових уразливостей та кібератак. Оновлення безпеки є ключовим для забезпечення захисту даних користувачів та інформаційної системи в цілому.

Оптимізація та вдосконалення. Оптимізація роботи ПЗ потрібна для покращення його продуктивності та вдосконалення функціональності відповідно до змінюваних вимог користувачів.

Підтримка користувачів. Надання допомоги та консультацій користувачам стосовно використання ПЗ, включаючи вирішення технічних проблем та відповіді на запитання.

Моніторинг системи. Постійний моніторинг стану ПЗ для виявлення та реагування на потенційні проблеми безпеки та продуктивності.

Документація та звітність. Створення та оновлення документації для ПЗ, включаючи керівництва користувача, технічні вказівки та звіти про оновлення безпеки.

Технічна підтримка та обслуговування є невід'ємною частиною життєвого циклу розроблення ПЗ, що гарантує його надійність, безпеку та ефективність на всіх етапах експлуатації.

Отже, ключовими принципами SSDLC є превентивні заходи, мінімізація ризиків на ранніх етапах, безперервна інтеграція безпеки, а також навчання та свідомість команди розробників щодо питань безпеки.

4.7. Автоматизація управління правами користувачів IT-систем як засіб підвищення ефективності інформаційної та кібербезпеки

Цифрова революція докорінно змінила вигляд робочого місця працівника будь-якої організації. Сьогодні жодне робоче місце не обходиться без використання інформаційних технологій. Ба більше, інформаційні технології дедалі глибше інтегруються в наше життя й потребують наявності комп'ютеризованої техніки [74]. Сучасна організація середнього або великого розміру зазвичай має до 10 систем критичного рівня та 20–30 систем локального обслуговування. Кожна з таких систем потребує адміністрування, насамперед обліку користувачів, які мають до них доступ.

4.7.1. Управління доступом до критичних корпоративних систем

Типовими прикладами таких систем критичного рівня є:

Microsoft AD (Active Directory), LDAP (Lightweight Directory Access Protocol) – система облікових записів користувачів;

SAP, MeDoc – бухгалтерський облік;

SAP HR, Talent Management System – системи кадрового обліку;

Megapolis Docnet, SharePoint – системи документообігу та файлового обміну;

Jira, Confluence, MS Project – системи управління проєктами та завданнями;

MS exchange – корпоративна пошта;

CRM – системи обслуговування клієнтів;

ServiceDesk – системи обслуговування звернень;

складський облік;

управління бізнесом та аналітика.

Корпоративні системи активно використовуються працівниками в щоденній роботі. А для забезпечення їхнього коректного функціонування використовується значна кількість програмно-апаратних комплексів, включаючи:

- ОС Window, Linux, Unix і т. п.;
- системи моніторингу IT-інфраструктури;

- ММЕ для віддалених користувачів, підключень відділень, у т. ч. хмарної інфраструктури;
- засоби віртуалізації, гіпервізори тощо.

Для ефективної роботи працівнику потрібен доступ до систем, які передбачені його посадою. Різним працівникам надається доступ до різного набору систем із різними правами доступу (рис. 4.8).

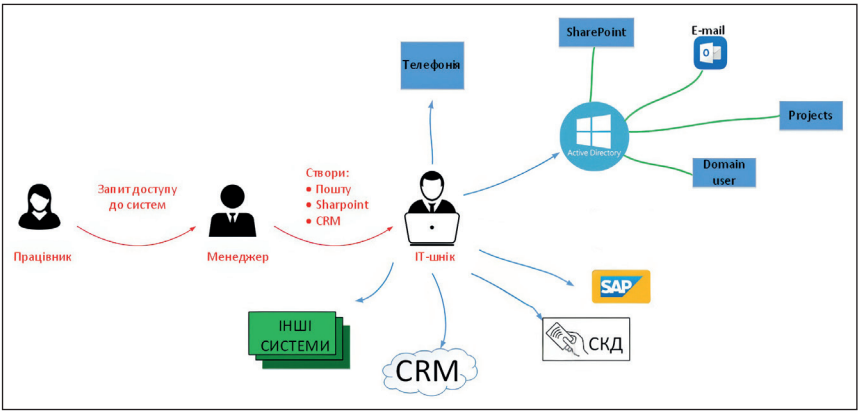

Рис. 4.8. Набір систем із різними правами доступу

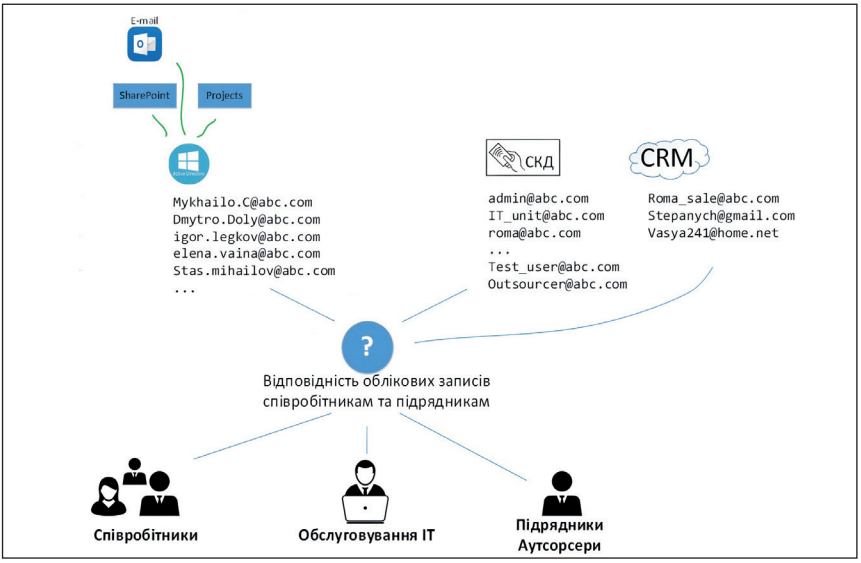

Рис. 4.9. Ідентифікація створених облікових записів на системах

Управління та контроль обліковими записами користувачів у корпоративних системах – серйозне завдання для підрозділу IT чи інформаційної та кібербезпеки [75]. Оскільки системи слабо інтегровані між собою, кожна потребує окремого налаштування облікових записів користувачів та відповідні права доступу. Створення, зміна та видалення прав доступу до кожної із цільових систем – це тривале й серйозне завдання для IT-підрозділу.

Ще складнішим є завдання ідентифікувати створені облікові записи на системах, визначити їх власників, класифікувати рівні прав доступу, а тим більше – виявити випадки перевищення прав доступу до систем та здійснити подальшу перевірку відповідності дозволеного й фактичного рівнів доступу до цільових систем (рис. 4.9).

4.7.2. Напрямки діяльності в управлінні доступом

Можна виділити три основні напрямки в управлінні доступом до критичних корпоративних систем:

- ідентифікація облікових записів систем – облікові записи важко однозначно «прив'язати» до працівника. Як «Login ID» використовуються скорочені імена чи прізвища, однак їх неможливо зв'язати із працівником компанії;
- управління обліковими записами користувачів – робота IT-підрозділу з налаштування корпоративних систем, надання доступу, змін доступу в разі зміни посадових обов'язків чи звільнення працівника;
- відповідність вимогам (compliance) – робота служби інформаційної безпеки з виявлення порушень прав доступу, регулярних перевірок налаштованих прав доступу, забезпечення авторизованого процесу затвердження прав доступу.

Для невеликих організацій, у яких керівник особисто знає свого працівника, чи для організацій із невеликим і сталим колективом актуальність управління обліковими записами користувачів невисока. Проте для організацій із кількістю користувачів 500 та більше налаштування доступів користувачів до кінцевих систем – це серйозне завдання, яке потребує окремого штату людей – IT-адміністраторів. У «просунутих» організаціях цей процес супроводжується оформленням заявок на обслуговування в системі service-desk [76].

Практичний досвід показує, що обслуговування облікових записів користувачів в організації із 4 000 працівників потребує формування підрозділу із 5–15 працівників. Завдання аудиту та ідентифікації облі-

кових записів по системах для такої організації настільки трудомістке, що потребує формування окремого проєкту обстеження для підрозділу інформаційної та кібербезпеки.

Не менш критичним завданням є проведення аудиту облікових записів користувачів, їхніх прав доступу до систем, визначення відповідальних осіб, які погоджували надання доступу. На практиці це виглядає так: працівник або його керівник ініціює звернення до підрозділу IT або до інформаційної та кібербезпеки щодо надання доступу до тієї чи іншої системи. Протягом деякого часу працівнику створюють обліковий запис у системі та встановлюють одноразовий пароль. Завершальний крок при видачі доступу – заміна користувачем одноразового паролю на власний.

Складніша ситуація із працівниками, які йдуть з організації. Оскільки контроль неактивних користувачів ускладнений, як правило, облікові записи колишніх працівників залишаються активними ще тривалий термін. Такі ситуації створюють суттєву загрозу інформаційній безпеці, оскільки облікові записи «без власників» вразливі до зламів. Оскільки обліковий запис не заблокований і в нього немає власника, його компрометацію важко виявити стандартними інструментами – легітимний користувач отримує доступ до системи. Важко запідозрити компрометацію облікових записів у масштабах 1 000 легітимних користувачів. Тому для підрозділу інформаційної та кібербезпеки важливою є так звана сертифікація користувачів – оперативні та регулярні перевірки відповідності фактично наданих прав внутрішнім чи зовнішнім вимогам.

4.7.3. Автоматизація управління правами доступу

Як правило, процес отримання доступу до корпоративних систем чітко регламентований [77]. Керівник структурного підрозділу ініціює запит до відповідних спеціалістів на надання доступу до певного корпоративного сервісу, який необхідний працівникам з його відділу. Якщо система критична чи знаходиться під управлінням сусіднього підрозділу – запускається процес погодження доступу до такої системи. Зазвичай у форматі електронного листування.

Оскільки за роботу систем в організації відповідають різні підрозділи, для організації доступу до таких систем необхідно задіяти декількох спеціалістів, а часто – декілька підрозділів. З метою фіксації події з видачі нових прав користувачам усі дії зі створення чи зміни облікових записів фіксуються в електронному листуванні або у service-desk-системах. Оскільки відповідальні профільні спеціалісти,

як правило, зайняті поточними завданнями, відпрацювання запитів триває від декількох годин до декількох тижнів. Весь процес роботи з обліковими записами створює значні затримки та додаткові завдання в повсякденній роботі працівників та IT-спеціалістів.

Сучасна концепція роботи з корпоративними системами полягає у формуванні сервісної моделі на базі використовуваних корпоративних систем. З точки зору сервісної моделі, організація надає працівнику певний сервіс на базі існуючих корпоративних систем. Прикладом корпоративного сервісу можуть бути доступи до:

- корпоративної пошти;
- мережі Інтернет;
- системи CRM;
- системи ERP;
- тощо.

У більш розвинутій сервісній моделі є можливим навіть такий поділ сервісів:

- необмежений доступ до мережі Інтернет;
- доступ до мережі Інтернет з обмеженням (Facebook, YouTube тощо);
- доступ до мережі Інтернет з 9:00 до 18:00.

Працівник чи його керівник знає, які сервіси йому необхідні для роботи. Тому, маючи можливість «замовити» відповідні сервіси, працівник автоматично запускає процедуру погодження доступу чи, якщо доступ надано, автоматично запускає механізм налаштування доступу до сервісу.

Кроком уперед в автоматизації управління доступом є створення порталів самообслуговування, де працівник може ознайомитись із переліком корпоративних сервісів, доступних для нього, та запросити до них доступ в автоматизованому режимі. При замовленні працівником доступних йому сервісів автоматично запускається процес погодження доступу до тих чи інших систем відповідальній особі. Відповідальна особа чи колектив осіб авторизує надання доступу. У такій системі можливо реалізувати процес багатовекторного погодження доступу, де декілька людей повинні погодити (не заперечувати) отримання доступу до системи.

Завдяки такій автоматизації працівник підрозділу інформаційної та кібербезпеки має змогу втрутитися в процес, зупинити погодження сервісу, переглянути обґрунтування надання сервісу та інше. Результати погодження будуть зафіксовані та збережені для подальшого опрацювання.

Одне із ключових завдань підрозділу інформаційної та кібербезпеки – аудит доступних сервісів (контроль правильності виданих доступів по системах). Хто, до яких систем, який доступ має і хто йому цей доступ затвердив? Як перевірити рівні доступів усіх користувачів на всіх системах як на рівні додатків, так і на рівні ОС?

Зібрати та підсумувати таку інформацію видається складним завданням, оскільки кількість та різноманітність систем організації така, що потребує проєктної команди для виконання цього завдання в обмежений термін. А після збирання та об'єднання інформації по користувачах та системах важливо зрозуміти, який обліковий запис, якому працівнику належить із подальшим визначенням правомірності виданого доступу.

Організація ефективного управління правами користувачів у корпоративних ІТ-системах, безумовно, вимагає автоматизації цього процесу, тому що вона несе в собі нові можливості для бізнесу. Це – створення процесу замовлення та затвердження прав доступу користувачів, створення порталу самообслуговування, формування вимог до облікових записів та створення відповідних інструментів контролю, перевірка відповідності наданих прав внутрішнім чи зовнішнім регуляторам, аудит видачі та затвердження прав доступу.

Отже, автоматизація процесу видачі та зміни облікових записів користувачів на корпоративних ІТ-системах дозволить скоротити час створення чи зміни прав доступу, створить передумови для контролю прав доступу до систем організації та підвищить ефективність роботи підрозділу ІТ або інформаційної та кібербезпеки в цілому.

4.8. Особливості забезпечення інформаційної та кібербезпеки в корпоративній мережі при віддаленому доступі

В умовах карантинних обмежень пандемії, а пізніше – введення воєнного стану в країні кардинально змінився підхід до використання інформаційних ресурсів. Переважна більшість організацій, які продовжили свою діяльність, змушені були перевести співробітників на віддалений режим роботи, що, у свою чергу, спричинило зміни в ІТ-інфраструктурі: збільшення навантаження на фаєрволи, мережеве обладнання та сервери, що обробляють зовнішні підключення. Організації, які до початку карантину обробляли інформацію виключно в локальній обчислювальній мережі, тепер змушені надавати доступ до своїх внутрішніх інформаційних ресурсів співробітникам, які працюють віддалено. З одного боку, можливість віддаленої роботи стала певною мірою панацеєю,

коли організації отримали шанс продовжувати роботу завдяки можливостям віддаленого доступу, обміну та обробки інформацією, з іншого – віддалений режим збільшив кількість векторів атаки на корпоративні ресурси [78].

Основне питання, яке виникло при переході на віддалений режим роботи – чи витримає збільшене навантаження обладнання локальних провайдерів і мобільних операторів? Збільшення трафіку дійсно відбулося, але, за інформацією від провідних телекомунікаційних операторів, завантаження не перевищило піковий трафік на новорічні свята. Тому обладнання провайдерів не є вузьким місцем при організації віддаленого доступу користувачів до корпоративної інформаційної мережі. Питання можуть виникнути щодо прикордонного мережевого обладнання, встановленого на стороні організації, та обмеження ширини каналу, що орендується у провайдера.

При переході на віддалений режим роботи зросла потреба в суворій багатофакторній аутентифікації віддалених користувачів для виключення можливості доступу до конфіденційної інформації неавторизованими особами. Функціонал цих рішень досить широкий і дозволяє забезпечити авторизацію користувача практично в будь-якій корпоративній ІС. Як фактори аутентифікації користувача можуть використовуватися: ключі-токени; смарт-карти; сертифікати, записані на носії; біометрія, прив'язана до конкретних користувачів; програмно-генеровані одноразові ключі тощо. Також використання цих рішень дозволяє створювати звіти про те, який користувач, коли і за допомогою чого отримав доступ до корпоративних інформаційних ресурсів.

Для забезпечення захисту корпоративних ресурсів за допомогою мультифакторної аутентифікації можна рекомендувати продукт ESET Secure Authentication (ESA), який відповідає вимогам корпоративної інформаційної та кібербезпеки й відрізняється простотою впровадження. ESA додає 2FA (двофакторна аутентифікація) в доменах MAD або в локальних комп'ютерних мережах, тобто створюється або OTP (One Time Password), який потрібно вказати разом зі звичайним ім'ям користувача і паролем, або push-повідомлення, у якому користувач на своєму мобільному телефоні під управлінням ОС Android, iOS або Windows після успішної аутентифікації за допомогою звичайних облікових даних для доступу повинен надіслати підтвердження [79].

Для роботи push-повідомлень потрібна ОС Android 4.0.3 або пізнішої версії, а також служби Google Play версії 10.2.6 або пізнішої версії, або iOS.

ESA складається з таких компонентів:

- підключається модуль ESA Web Application (вебдодаток ESA), що забезпечує двофакторну аутентифікацію (2FA) в різних вебдодатках Microsoft (Microsoft Web Applications);
- підключається модуль ESA Remote Desktop (віддаленого робочого столу ESA), що забезпечує двофакторну аутентифікацію для протоколу віддаленого робочого столу RDP (Remote Desktop Protocol);
- підключається модуль ESA Windows Login, що надає двофакторну аутентифікацію для комп'ютерів з ОС Windows;
- сервер ESA RADIUS Server додає двофакторну аутентифікацію в аутентифікацію VPN;
- служба ESA Authentication Service (служба аутентифікації ESA) включає інтерфейс API, який заснований на архітектурі REST і за допомогою якого можна додавати двофакторну аутентифікацію в користувацькі додатки.

ESA Management Tools (засоби управління ESA):

➢ При встановленні ESA в середовищі Active Directory

- підключається модуль управління користувачами ESA User Management (управління користувачами ESA) для засобу ADUC (Active Directory Users and Computers) (користувачі та комп'ютери AD), що використовується для управління користувачами;
- консоль управління ESA (ESA Management Console), яка називається ESET Secure Authentication Settings і використовується для налаштування ESA;
- вебконсоль ESA є багатофункціональним засобом управління, який також можна використовувати для налаштування ESA й управління користувачами.

➢ При встановленні ESA в режимі окремого сервера

- вебконсоль ESA є багатофункціональним засобом управління, який використовується для налаштування ESA та управління користувачами.

Якщо ESA встановлено в середовищі AD, то це рішення зберігає дані в сховищі даних AD. Оскільки дані ESA автоматично додаються до резервних копій AD, немає необхідності в додаткових політиках резервного копіювання.

Для встановлення ESA потрібен домен AD або локальна мережа. Мінімальний підтримуваний функціональний рівень домену AD – це Windows 2000 Native. Підтримується лише Windows DNS. Як альтернативу ESA можна використовувати продукт One Identity Defender, який

дозволить значно підвищити безпеку корпоративних інформаційних систем при віддаленому доступі і відповідає всім міжнародним стандартам безпеки. One Identity скорочує час узгодження процесів, з якими пов'язане управління ролями та управління доступом звичайних і привілейованих користувачів; покращує гнучкість прийняття рішень в організаціях, а також вирішує проблеми, пов'язані з управлінням ролями та доступом користувачів в on-premise хмарному або гібридному середовищі.

За допомогою One Identity Defender можна [80]:

- визначати точні кроки для забезпечення управління ролями та доступом користувачів;
- дати можливість бізнес-користувачам приймати рішення про надання доступу;
- доопрацьовувати компоненти рішення для відповідності завданням;
- розгортати рішення для управління ролями та доступом користувачів і почати окупати інвестиції в рішення протягом декількох тижнів;
- впровадити рішення, яке дозволить прискорити прийняття рішень в організації;
- отримати повне управління ролями, даними та доступом користувачів, орієнтоване на бізнес, об'єднавши контроль, повну видимість та адміністрування;
- забезпечити всіх користувачів організації доступом до необхідних їм ресурсів із будь-якого пристрою і в будь-якому місці – безпечно, просто і відповідно до всіх стандартів;
- автоматизувати створення облікових записів, надання доступу, спростити адміністрування процесами, а також об'єднати ролі, паролі і каталоги за допомогою поліпшених можливостей з управління доступом;
- управляти привілейованими обліковими записами користувачів централізовано, проактивно, фокусуючись на відповідальності окремих користувачів за допомогою гранулярного контролю і моніторингу доступу адміністраторів;
- отримати можливості з управління ролями та доступом користувачів в організації без необхідності капітальних вкладень в обладнання або труднощів, пов'язаних із розрахунком користувачів;
- вивільнити ресурси help desk за допомогою порталу самообслуговування.

Однак навіть при дотриманні суворої мультифакторної аутентифікації користувача все одно залишається потреба в контролі використання

конфіденційної інформації. У сучасних умовах інформація дублюється на корпоративних і домашніх пристроях, а BYOD збільшує ризик витоку. Корпоративна переписка доступна на робочому ПК, на домашньому ПК, на особистому або корпоративному смартфоні.

Зростання вартості інформації та збільшення кількості інцидентів змушують служби інформаційної і кібербезпеки більш ретельно контролювати системи, на яких відбуваються обробка та зберігання інформації. Це можливо за допомогою рішень DLP, MDM і PAM.

DLP-система являє собою спеціалізоване ПЗ, призначене для захисту компанії від витоків інформації [81]. Вони діляться на системи з активним і пасивним контролем, що встановлюється над діями користувача. Активні мають таку здатність, пасивні – ні. Перші – більш ефективні, оскільки запобігають витоку інформації, блокуючи дії користувачів або роботу ПЗ при виявленні інциденту. З іншого боку, у них є недолік – технологія може мимоволі порушити якийсь критичний бізнес-процес. З пасивними такого не відбувається, вони використовуються для профілактики систематичних витоків із реагуванням постфактум.

За класифікацією, побудованою на мережевій архітектурі, DLP-рішення бувають шлюзовими і хостовими. Перші функціонують на серверах, а другі застосовують на робочих станціях користувачів. Багато сучасних DLP поєднують обидва способи контролю – так вдається досягти високих показників їх ефективності.

Крім основної функції забезпечення інформаційної і кібербезпеки, технологія запобігання витокам допомагає вирішувати й інші завдання щодо встановлення контролю над діями співробітників організації. До прикладів їх застосування належать:

- облік робочого часу, а також використання ресурсів;
- аналіз правомірності дій працівників із метою мінімізації ризику виготовлення підроблених документів;
- виявлення ознак так званої підкилимової боротьби, яка може завдати шкоди організації, через моніторинг спілкування та взаємодії між співробітниками;
- виявлення співробітників, які планують зміну роботи, для швидкого пошуку нових фахівців, мінімізації ризику витоку даних разом із кадрами, що звільняються.

Ці рішення дозволяють вирішувати безліч важливих завдань і, по суті, є ефективним інструментом, що забезпечує інформаційну і кібербезпеку. Для великих компаній, безумовно, цікавими є повноцінні рішення, що поєднують в собі функціонал HostDLP і NetworkDLP, такі

як DigitalGuardian DLP, Mcafee DLP, Symantec DLP. Середньому бізнесу можна рекомендувати так звані рішення «офісного контролю», де можливість контролю й недопущення витоку конфіденційної інформації поєднана із загальним моніторингом дій користувача і дозволяє об'єктивно оцінювати використання співробітником робочого часу. До них відносяться EndpointProtector від компанії CoSoSys, Safetica DLP від компанії ESET, а особливої уваги заслуговує Mirobase, який уже понад сім років представлений на ринку України і за цей час був упроваджений у великій кількості корпоративних ІС.

Для управління основними даними необхідно використовувати системи MDM (Master Data Management), які являють собою сукупність процесів та інструментів, що використовуються для здійснення безперервного управління основними даними організації, у тому числі довідковими [82]. Термін MDM є досить широким. Загальне призначення таких систем – управління мобільними пристроями, які мають доступ до IT-інфраструктури організації. Однак ключове завдання, яке вони вирішують, – управління не стільки самими пристроями, скільки додатками, які на них встановлені. Звідси походить найважливіша функція MDM-систем – саме через додатки можна отримати доступ до інформації всередині «периметра» організації. У них шукають «дірки» зловмисники. Через додатки відбувається ненавмисний витік даних через неакуратність користувачів.

Сучасні MDM-рішення вирішують кілька завдань. Організація захищає всі «точки доступу» до корпоративної інформації і веде пошук можливих загроз. Співробітники організації отримують доступ до різних корпоративних сервісів, починаючи з електронної пошти й месенджерів і закінчуючи корпоративними системами. Система контролює і використання даних у віддаленому режимі. Також за допомогою MDM можна організувати дистанційну підтримку користувачів – допомагати їм із налаштуваннями пристроїв, установленням або оновленням додатків. Таким чином, MDM-система дає корпоративним IT-службам досить широкі можливості:

- дозволяє встановлення на пристрої й видалення додатків і сертифікатів безпеки;
- забороняє використовувати ненадійні додатки та сервіси;
- дозволяє віддалене налаштування пристрою відповідно до прийнятих у компанії політик;
- допускає шифрування даних на пристрої;
- забезпечує роботу із втраченими пристроями: пошук їхньо-

го місцезнаходження, блокування, знищення конфіденційних даних у пам'яті.

В умовах віддаленої роботи збільшився попит на системи надання та контролю доступу привілейованих користувачів, оскільки необхідно організувати та контролювати роботу технічних фахівців, системних адміністраторів та хелпдеску, який продовжує обслуговувати критично важливі вузли IT-інфраструктури.

PAM – це набір модулів, які відповідають за аутентифікацію в системі. По суті, це API, який ОС або додатки можуть використовувати, щоб відправити запити на перевірку аутентичності користувача. PAM розшифровується як Pluggable Authentication Modules – підключувані модулі аутентифікації [83]. PAM розроблена компанією Sun Microsystems і була представлена в 1995 році. Раніше в UNIX за авторизацію користувача в систему відповідала програма login, яка приймала логін та пароль і порівнювала дані з даними у файлі /etc/passwd. Наразі login не займається аутентифікацією, а просто передає завдання PAM, який за допомогою набору своїх або додатково підключених алгоритмів перевіряє аутентичність користувача і повертає відповідь. Даний модуль можна зустріти в багатьох ОС на основі UNIX, наприклад, Ubuntu, CentOS, Debian, Red Hat, FreeBSD, Gentoo, Mac OS X, Solaris і багатьох інших. Налаштування PAM виконується в головному конфігураційному файлі /etc/pam.conf і підключених із каталогу /etc/pam.d, назва кожного файлу в якому точно відповідає назві програми, яка використовує модуль pam для аутентифікації. У деяких системах, наприклад, Linux CentOS, файлу pam.conf може і не бути – налаштування виконується за допомогою файлів у pam.d. У цілому рішення PAM дозволяють забезпечити безпечне й контрольоване підключення технічних фахівців до вузлів IT-інфраструктури організації.

В умовах віддаленої роботи зросли загрози з боку вірусного ПЗ. Найчастіше віддалене підключення відбувається з домашніх ПК, на які не поширюються політики безпеки та корпоративні антивірусні рішення. Захист віддалених персональних робочих станцій може бути реалізований різними методами [84]. Найпростішим рішенням вважається використання корпоративного антивірусу ESET із системою управління ліцензіями. На час карантину ESET надає тимчасові ліцензії для встановлення на домашні ПК співробітників організації. Схеми побудови периметра безпеки можуть відрізнятися внаслідок відмінностей ІС організацій. Можлива реалізація через клієнтів Endpoint Security Client, які надають безпечне VPN-з'єднання.

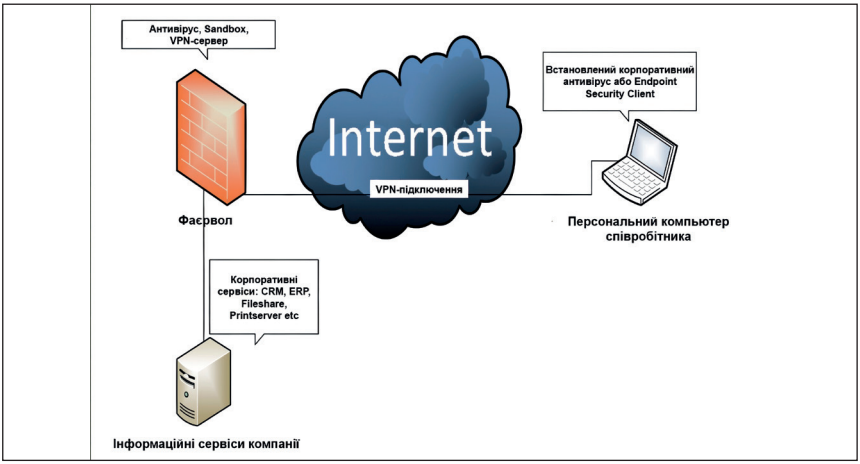

Рис. 4.10. Схема побудови захисту віддалених робочих станцій

Такі рішення пропонують компанії FortiNet, Sophos, CheckPoint. Основна відмінність клієнтів від антивірусних рішень полягає в неможливості працювати в режимі standalone, тобто без підключення до керуючого сервера, який знаходиться в корпоративній IT-інфраструктурі.

Різновидом віддаленої роботи є проведення вебконференцій або конфколів. Такий формат взаємодії дозволяє в режимі реального часу проводити збори географічно віддалених співробітників. На жаль, деякі системи організації вебконференцій опинилися в центрі скандалів, пов'язаних із викраденням записів минулих корпоративних вебконференцій і витоком корпоративних акаунтів. Так, 14 квітня 2020 року була опублікована новина про те, що на ресурсах у Darknet продається понад пів мільйона користувацьких облікових записів Zoom. Понад десять тисяч відеодзвінків, зроблених через Zoom, були опубліковані на YouTube і Vimeo. У мережі опинилися записи сеансів психотерапії, шкільні уроки, консультації з лікарями та бізнес-зустрічі, на яких обговорювалася фінансова звітність. Zoom не записує переговори за замовчуванням, але організатори онлайн-конференцій можуть увімкнути запис і зберегти його безпосередньо в Zoom або окремо, на своїх персональних комп'ютерах, без згоди інших учасників. Канали витоку не визначені. Zoom присвоює відеоконференціям відкриті ідентифікатори і не шифрує підключення. В онлайн-пошукових системах можна знайти понад 15 000 записів. Із цієї причини ряд великих компаній, таких як Google і Samsung, а також деякі державні організації США і ЄС, були змушені заборонити своїм

співробітникам використовувати Zoom у роботі. Захищений сервіс, який дозволить забезпечити стабільний зв'язок під час вебконференції та захистити запис – Cisco Webex. В умовах карантину компанія Cisco надає безкоштовну 90-денну ліцензію для підтримки бізнесу в умовах карантину.

Отже, зміна процесів роботи в корпоративних ІС показала актуальність і необхідність посилення заходів для забезпечення інформаційної і кібербезпеки при застосуванні віддаленого доступу для можливості розподіленої роботи співробітників і забезпечення вільного переміщення інформації в корпоративній мережі з високою швидкістю її поширення. З іншого боку, ці зміни несуть і нові загрози: ослаблення контролю доступу до інформації, її неконтрольоване поширення, складність оцінки важливості інформації в динамічно мінливих умовах. Ефективно протистояти виниклим загрозам можна, використовуючи системи мультифакторної аутентифікації та шифрування, DLP, MDM, PAM і системи відеоконференцій. У цьому випадку комунікація між користувачами корпоративної ІС мережі буде швидкою й захищеною.

4.9. Забезпечення кібербезпеки при використанні технології Інтернету речей

Упродовж останніх років з'явилися нові пристрої, під'єднані до Інтернету та об'єднані в різні групи, що отримало назву Internet of Things (IoT) [85]. Здебільшого це побутові або промислові пристрої, які для управління або обміну інформацією мають можливість підключення до Інтернету або до сервера управління й контролю через Інтернет. Такий пристрій, під'єднаний до мережі, є практично не захищеним, а тому привабливим для різного роду кіберзловмисників, тож проблема забезпечення кібербезпеки IoT-пристроїв є дуже актуальною. Для розв'язання цієї проблеми потрібно проаналізувати особливості IoT-пристроїв у контексті їх використання як масового способу зараження вірусами інформаційних систем та розробити рекомендації щодо забезпечення безпеки [86].

За даними Statista, зараз у світі понад 51 млрд під'єднаних пристроїв, а до кінця 2025 року їх буде понад 75 млрд (рис. 4.11). Уже зараз кількість під'єднаних пристроїв перевищує кількість людей на Землі (7,5 млрд осіб) у 8 разів, а у 2025 році перевищить майже в 10 разів. Тому ігнорувати питання безпеки десятків мільярдів пристроїв, незважаючи на те, що кожен із них є маловиробничим, було б хибно [87–90].

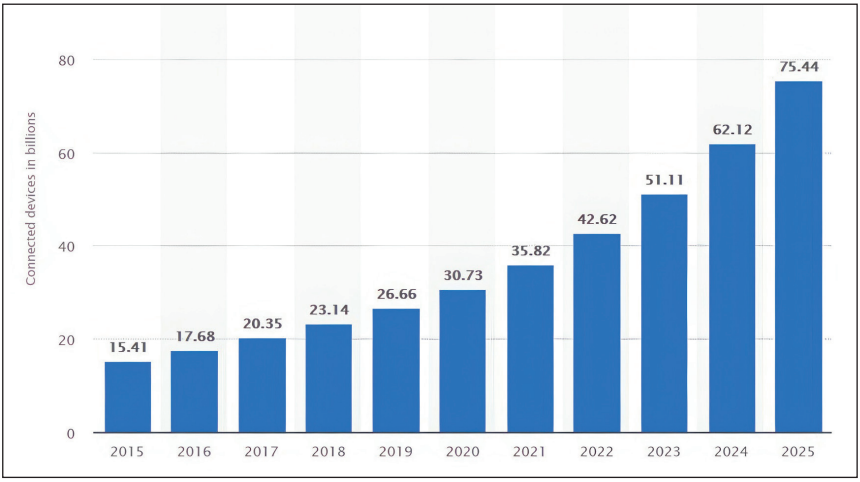

Рис. 4.11. Динаміка збільшення IoT-пристроїв

Ці спеціалізовані пристрої з підключенням до мережі (дротовим або бездротовим) мають низку особливостей. Перша – це невисока обчислювальна потужність, невеликий обсяг пам'яті та обмежений набір виконуваних команд. Другою особливістю є те, що користувач, який експлуатує IoT-пристрій, не є фахівцем у сфері інформаційних технологій або експертом із кібербезпеки і, відповідно, не може правильно налаштувати IoT-пристрій для безпечної роботи в мережі. Саме тому він має бути спочатку налаштований виробником і керуватися ним під час експлуатації, інакше IoT-пристрій може стати потенційним джерелом мережевих проблем.

Третя особливість – IoT-пристрій немає серйозного функціоналу безпеки, тому що будь-які обмежувальні налаштування можуть створити труднощі під час експлуатації непідготовленими користувачами.

Обмеження, що накладаються на мережеву взаємодію IoT-пристрою, можуть призвести до того, що конфігурація налаштувань пристрою та його мережеве оточення виявляться несумісними, і доступ до мережі не буде встановлено. Саме тому виробники намагаються зробити кількість обмежень якомога меншою, а мережеві налаштування якомога простішими.

Включення будь-якого IoT-пристрою в бот-мережу відбувається після зараження його вірусом. IoT-пристрої зазвичай мають справу з вірусом сімейства Mirai (за ім'ям бінарного файлу) або подібним до нього. Він атакує Linux-пристрої з набором утиліт Busybox. Вірус намагаєть-

ся отримати доступ до IoT-пристрою через telnet (так звана соціальна інженерія), перебираючи 50 варіантів імен / паролів, які використовують за замовчуванням в IoT-пристроях найбільші виробники (Ubiquiti, Raspberry, Ubuntu based, Dahua, Hikvision та ін.).

Щойно доступ до IoT-пристрою отримано, вірус інсталюється в систему, зв'язується з контролером ботнету, повідомляє про себе; далі видаляється з носія для зменшення ймовірності виявлення, залишаючись в оперативній пам'яті; сканує діапазон IP-адрес, перевіряючи наявність вразливих пристроїв, та надсилає цю інформацію контролеру ботнету. Незважаючи на те, що вірус є досить простим і використовує звичайний метод повного перебору пароля brut force, але, як виявилося, і цього достатньо для організації ботнету на сотні тисяч IoT-пристроїв.

Зараз нові зараження вірусом Mirai виникають дедалі рідше, але це не означає, що його переможено. По-перше, існує безліч мутацій і варіантів вірусу (Hajime, LuaBot тощо), а по-друге, IoT-пристрій, який перетворено на складову ботнету, жодним чином себе не проявляє і використовується контролером ботнету для подальших атак. Тобто можна тільки припускати, наскільки вірус розповсюдився та яку кількість пристроїв він контролює.

Позбутися вірусу Mirai та запобігти подальшому зараженню досить просто. Для цього потрібно від'єднати IoT-пристрій від Інтернету, перезавантажити його, поміняти ім'я / пароль на стійкі до злому, за можливості заборонити під'єднання до пристрою через Інтернет за допомогою telnet / ssh та іншими можливими способами, а потім під'єднати пристрій до Інтернету знову.

Ще однією рекомендацією буде перевірити наявність ПЗ і встановити його оновлення. Зниження активності вірусу Mirai відбувається завдяки тому, що «кормова база» вірусу зменшується, а саме: IoT-пристрої, заражені одним контролером ботнету, не піддаються зараженню іншим, а після завершення атаки контролер вимикають, і мережа залишається в пасивному стані. Крім того, кількість незахищених IoT-пристроїв зменшується завдяки виконанню рекомендацій із кібербезпеки.

Це свідчить про фактично нульовий рівень кібербезпеки IoT-пристроїв, оскільки навіть такий нескладний вірус, який отримує доступ до пристрою за допомогою простого перебору 50 паролів за замовчуванням, може проникнути в сотні тисяч IoT-пристроїв і виконати шкідливі дії. Проблема також і в тому, що власники таких IoT-пристроїв навіть не підозрюють, що їхній пристрій зазнав атаки, бо проблеми виникають не в них.

Існує ще один клас вірусів – BrickerBot. Наразі він представлений двома версіями: BrickerBot.1, BrickerBot.2. Вірус було виявлено й описано компанією Radware навесні 2017-го. Результатом дії цих вірусів є PDoS (Permanent Denial of Service), а саме неможливість використання цього пристрою, перетворення його на цеглу (назва вірусу походить від англ. Brick – цегла). Вірус атакує IoT-пристрої на базі Linux із набором Busybox (рис. 4.12).

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Рис. 4.12. Атака вірусу BrickerBot.1

Під час атаки перевіряється відкритий TCP-порт 23 (telnet) і відбувається підбір пароля, починаючи з пари ‘root’/’vizxv’. У цьому BrickerBot повністю схожий на вірус Mirai. Розбіжності полягають у діях вірусу після проникнення. BrickerBot виправдовує свою назву. Він намагається видалити весь вміст будь-якого сховища – внутрішнього або безпосередньо підключеного до пристрою, порушує зв’язок з Інтернетом (net.ipv4.tcp_timestamps=0) і перешкоджає виконанню операцій ядра (kernel.threads-max=1). Таким чином цей вірус, по суті, робить IoT-пристрій недоступним, що призводить або до заміни пристрою, або до повного його обнулення й відновлення прошивки.

Різниця між BrickerBot.1 і BrickerBot.2 полягає в ініціаторах зараження, у способі дії після зараження та у тривалості атак. Якщо перший вірус атакував із певного набору IP-адрес, то другий – із мережі TOR, тому відстежити його ініціаторів не так просто. Крім того, він не використовує набір BusyBox, що робить його більш універсальним.

Існує думка, що BrickerBot.2 активний і досі. Переважна більшість фахівців вважає, що BrickerBot запустили для зменшення кількості IoT-пристроїв, доступних для атаки вірусів типу Mirai, оскільки оби-

два віруси використовують однакові алгоритми проникнення. BrickerBot просто знищує IoT-пристрій, який доступний для зараження Mirai. Є припущення, що вірус спочатку намагається допомогти зараженому пристрою, усунувши вразливості, нічого водночас не пошкоджуючи; якщо це не виходить, діє деструктивно. Але ці повідомлення поки що неможливо ні підтвердити, ні спростувати. Однак, незважаючи на такі, можливо, благородні поривання, вірус BrickerBot несе реальну загрозу безпеці та життю людей.

Уявімо, що виведено з ладу камери відеоспостереження, NVR-відеореєстратори на об'єктах критичної інфраструктури, медичне обладнання під час операції або системи управління тепло- та електропостачанням у зимовий період тощо. Звісно, перелік вірусів IoT-пристроїв не обмежується Mirai, Hajime, LuaBot, BrickerBot.1 та BrickerBot.2. Вони стали дуже відомими через суспільний резонанс, спричинений великими DDoS-атаками з масовим зараженням IoT-пристроїв.

Ускладнення способів атаки на IoT-пристрої сприяє появі нових можливостей отримання прибутку. Незахищеність побутових IoT-пристроїв і можливість електронних розрахунків приваблює кібершахраїв.

Уже були випадки експериментальних зломів домашніх регуляторів температури з блокуванням і вимогами оплати за розблокування (дія, аналогічна широковідомому в нашій країні вірусу Petya). Зважаючи на те, що в середньостатистичному будинку більшості країн підключено приблизно 12 IoT-пристроїв до Інтернету (зокрема, маршрутизатори, ТБ, холодильники, «розумний дім», термостати тощо), то знайти незахищений IoT-пристрій і, перехопивши керування ним, зажадати грошей, не буде чимось неможливим.

Говорячи про перехоплення управління, потрібно згадати про «розумні автомобілі». За повідомленнями ABI Research, у світі близько 100 млн зареєстрованих транспортних засобів, які в той чи інший спосіб під'єднано до Інтернету (для діагностики, оновлення дорожньої інформації тощо), а до 2030 року їхня кількість збільшиться до 400 млн (рис. 4.13). Вони також можуть стати об'єктом атаки, яка матиме катастрофічні наслідки.

Наприклад, уже було успішно перехоплено керування автомобілем Jeep Cherokee, заблоковано двері й відправлено машину в кювет разом із водієм. Атаку було здійснено через інформаційно-розважальну систему автомобіля, під'єднану до Інтернету.

Для розв'язання проблеми забезпечення кібербезпеки IoT-пристроїв рекомендується зробити такі кроки:

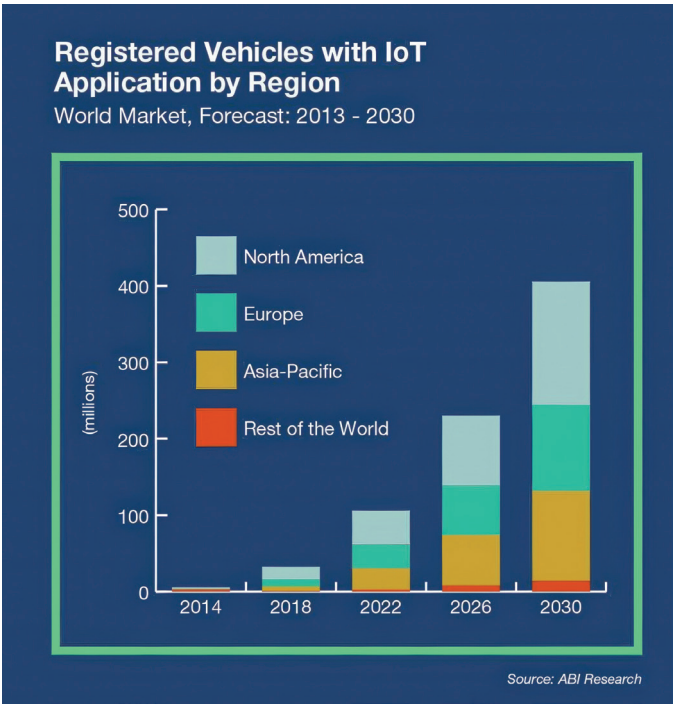

Рис. 4.13. Транспортні засоби з IoT-пристроями

- змінити ім'я / пароль пристрою на зламостійкий (вимога до пароля – щонайменше вісім символів, має містити цифри, літери верхнього регістру та спеціальні символи);
- встановити всі оновлення кібербезпеки виробника;
- перевірити репутацію виробника з погляду кібербезпеки;
- встановити всі оновлення кібербезпеки виробника;
- перевірити під час придбання IoT-пристрою репутацію виробника з огляду на кібербезпеку.

На сьогодні є чітке розуміння того, як реалізувати ці рекомендації в корпоративній мережі. Але це потрібно зробити й для кінцевого користувача, підключеного до Інтернету, у якого всі налаштування безпеки в кращому разі встановлено за замовчуванням, а в гіршому – відключено зовсім. Розв'язання цієї проблеми можливе лише за комплексного підходу, за якого користувач не відіграватиме ключову роль через брак необхідної компетенції. Отже, завдання забезпечення кібербезпеки IoT-пристроїв має дві складові: налаштування безпеки на самому пристрої та мережева безпека.

Унесення змін у налаштування й додавання функцій безпеки – завдання виробника. Ба більше, це стосується як нових IoT-пристроїв, на яких потрібно змінити налаштування за замовчуванням, так і наявних. Виробник має внести такі зміни на IoT-пристрої: встановити надійний пароль під час першого ввімкнення системи; встановити захист від повторного набору пароля (тайм-аут перед черговою спробою входу та блокування акаунта на час після трьох невдалих спроб); вимкнути за замовчуванням усі необов'язкові мережеві протоколи та зовнішній telnet; вимкнути Wi-Fi за замовчуванням та увімкнути його лише після налаштування безпеки WPA-PSK (Wi-Fi Protected Access-Pre-Shared Key) або WEP (Wired Equivalent Privacy).

Якщо виробник бере на себе всі функції забезпечення кібербезпеки, зокрема й мережевого периметра IoT-пристрою, то весь його трафік має проходити через Центр обробки даних (ЦОД), у якому буде передбачено захист від мережевих атак та вірусів. Для цього, після підключення до Інтернету, IoT-пристрій активує SSL-тунель (Secure Sockets Layer tunnel) на заздалегідь установлену адресу кластера концентраторів у ЦОД виробника, і будь-який інший трафік, крім трафіка VPN, у зовнішній простір забороняється. Діючи таким чином, виробник може на IoT-пристрої забезпечувати захист від зараження та мережевих атак; перевіряти стан і помилки на пристрої для проактивної підтримки; контролювати актуальність ПЗ і зміни налаштувань. Недоліком такого рішення є те, що весь трафік пристрою йде не за оптимальним маршрутом, тобто суттєво затримується, оскільки йому потрібно проходити через глобальний або регіональний ЦОД виробника.

Для виробника найбільш доцільно забезпечити мережеву безпеку IoT-пристроїв, які не використовують під'єднання до Інтернету для передання «важкого» контенту (відео, аудіо тощо). Так, деякі країни заборонили певні типи IoT-пристроїв через їхню небезпеку та вразливість до злому, що може спричинити тяжкі наслідки. У разі неможливості або неготовності виробника створити свій ЦОД із центром очищення трафіку, цю функцію може взяти на себе оператор зв'язку, який зазвичай володіє необхідними ресурсами, бо існує небезпека, що трафік оператора може бути заблоковано через великий потік DDoS-атак або інших з його IP-адрес.

Оператор зв'язку може пропускати весь трафік через мережеву систему безпеки і брати на себе такі функції: виділення трафіку IoT-пристроїв; перевірки трафіку IoT-пристроїв на віруси та аномалії трафіку за допомогою системи Advanced Mailware Protection; блокування трафіку

відомих контролерів ботнету. Крім того, може надати послугу з управління й контролю IoT-пристроями абонентів на базі сімейства протоколів TR-69, розмістивши у своїй корпоративній мережі сервер керування і передавши його адресу в налаштування абонентських IoT-пристроїв. У цьому разі постає питання безпеки самого сервера, контролю доступу до нього й захисту від шкідливого ПЗ, але ця проблема вирішується системою корпоративної інформаційної та кібербезпеки.

Для виконання цих заходів потрібно: виробнику вбудувати в IoT-пристрої фаєрволи, TR-69 і VPN-клієнти; змінити налаштування безпеки та ускладнити первісне налаштування IoT-пристроїв користувачем; побудувати ЦОД для забезпечення мережевої безпеки; встановити сервер керування; розширити службу підтримки виробників групою з проблем безпеки; оператору розширити свою підсистему malware protection; користувачу пройти складнішу процедуру налаштування IoT-пристроїв і витратити більше коштів на кібербезпеку. Однак витрати на ці заходи будуть дещо менші, ніж потенційні втрати від можливих DDoS-атак із використанням IoT-пристроїв як засобів масового зараження.

Отже, проведений аналіз проблеми використання IoT-пристроїв як дуже простого й масового способу зараження вірусами ІС підтверджує необхідність організації ефективної протидії цьому виду кіберзагроз. Розроблені рекомендації щодо забезпечення кібербезпеки IoT-пристроїв підтверджують, що такі можливості існують. Однак малоймовірно, що виробники IoT-пристроїв і тим більше оператори зв'язку захочуть самостійно вжити необхідних заходів для їхнього кіберзахисту. З огляду на всю серйозність такого виду кіберзагроз розв'язання регуляторних питань у цій сфері має взяти на себе держава, оскільки для забезпечення кібербезпеки під час масового використання IoT-пристроїв потрібно внести відповідні зміни до національної нормативно-правової бази.

4.10. Комплексний підхід щодо кібербезпеки систем промислового Інтернету речей

Поняття промислового Інтернету речей (Industrial Internet of Things, IIoT) уперше було озвучене в 2011 році в рамках Індустріальної революції 4.0, на міжнародній виставці в Ганновері, і стало підсумком діяльності німецьких науковців, які на рівні концепції поєднали використання великої кількості датчиків та контролерів, об'єднаних у мережу для досягнення певного виробничого результату [91].

IIoT – це концепція, яка поєднує в собі потужність глобальної інформаційної мережі та традиційної промисловості [92, 93]. Вона об'єднує новітні досягнення у сфері інформаційних та виробничих технологій, такі як ШІ, високошвидкісний обмін даними, бездротові технології, обробка великих обсягів інформації в режимі реального часу та багато іншого.

Сили кібероперацій різних країн, терористичні угруповання та злочинці цікавляться можливістю впливу на реальність за допомогою втручання в роботу глобальної інформаційної мережі і мереж IIoT, які є її частиною. Кількість втручань зростає щороку. Спочатку це виглядає як розвідка та з'ясування того, яка конфіденційна інформація може бути отримана, далі – отримання цієї інформації в режимі реального часу. Але згодом змінюються задачі та можливості впливу ІС. Перехоплення, керування військовими дронами, саботаж на транспортних шляхах та виробництві можуть призвести до реальних жертв, а не лише до фінансових та репутаційних збитків, як у випадку із втручанням в автоматизовані ІС. Промисловий Інтернет речей, незважаючи на всі свої переваги, стикається з низкою серйозних загроз, які можуть призвести до порушення виробничих процесів, значних фінансових втрат та навіть фізичної шкоди. Всесвітній економічний форум викликав певну тривогу, зазначивши, що «саме виробництво було найбільшим об'єктом для кібератак».

Компанія IBM підрахувала, що у 2022 році понад третину всіх спроб вимагання грошей кіберзлочинцями за розблокування даних була спрямована саме на виробничі підприємства. Це пояснюється тим, що такі підприємства не можуть дозволити собі тривалі простої. У свою чергу, компанія SonicWall повідомила, що у 2023 році кількість шкідливих програм, які атакують пристрої Інтернету речей, зросла на 37 %. Це означає, що хакери все частіше націлюються на різні пристрої, підключені до Інтернету, наприклад, датчики, контролери, камери та промислове обладнання.

4.10.1. Особливості систем IIoT

Сучасні виробничі підприємства все більше інтегрують цифрові технології, перетворюючись на складні системи, що поєднують фізичні та кібернетичні компоненти. Це підвищує ефективність виробництва, але водночас створює нові ризики, тому що системи IIoT набагато вразливіші до кібератак порівняно зі звичайними комп'ютерними мережами. І це відбувається внаслідок таких причин:

1. *Складність і масштабність*. Системи IIoT складаються з великої кількості взаємопов'язаних пристроїв – від датчиків і контролерів до роботів і систем автоматизації. Така масштабність ускладнює їхній захист, оскільки кожна нова ланка в системі може стати потенційною вразливістю.

2. *Різноманітність протоколів*. Різні пристрої в системах IIoT можуть використовувати різні комунікаційні протоколи, що ускладнює забезпечення єдиного рівня безпеки для всієї системи.

3. *Застаріле обладнання.* Багато промислових підприємств використовують обладнання, яке було встановлене багато років тому. Таке обладнання часто має вбудоване ПЗ зі значними вразливостями, якими можуть скористатися зловмисники.

4. *Недостатня увага до безпеки.* Історично склалося так, що безпека промислових систем часто відходила на другий план. Підприємства більше зосереджувалися на підвищенні продуктивності та зниженні витрат, ніж на захисті своїх систем від кібератак.

5. *Відсутність кваліфікованих фахівців*. Існує дефіцит фахівців із кібербезпеки, які мають досвід роботи з промисловими системами. Це ускладнює захист таких систем від кібератак.

6. *Відсутність єдиного стандарту безпеки.* На відміну від IT-інфраструктури, у промисловій автоматизації немає єдиного набору стандартів безпеки, що ускладнює забезпечення захисту. Наслідки кібератак на системи IIoT можуть бути катастрофічними й мати такі результати: зупинення виробництва; пошкодження обладнання; витік конфіденційної інформації про виробничі процеси, технології тощо; репутаційні втрати.

4.10.2. Способи атак на системи IIoT

Для здійснення атак на системи IIoT зловмисники намагаються проникнути в середину мережі. Вони можуть підібрати варіант проникнення всередину, використовуючи вади ПЗ, конфігурування системи, недостатню підготовку обслуговуючого персоналу або поєднати та комбінувати існуючі недоліки системи IIoT. Для досягнення своєї мети зловмисники використовують такі способи:

1. *Атака підбором паролів*. Слабкі паролі є легкою мішенню для зловмисників.

2. *Атака людини посередині*. Полягає в перехопленні даних між елементами системи та порушення цілісності даних, або ж маніпуляція

ними. Зміна даних, що передаються між пристроями, може призвести до прийняття помилкових рішень та пошкодження обладнання.

3. *Підробка ідентифікаторів*. Наявність проблем з аутентифікацією, що призведе до отримання несанкціонованого доступу до системи.

4. *Використання незахищених портів та протоколів.* Помилки в конфігурації пристроїв можуть створити вразливості, якими легко скористаються зловмисники.

5. *Пошук вразливостей ПЗ.* Застаріле ПЗ із відомими вразливостями, які не були виправлені, може бути легко зламане.

6. *Застосування комп'ютерних вірусів.* Наявність вірусної небезпеки призводить до того, що комп'ютерний вірус, розрахований на контролери та системи керування, може зіпсувати роботу обладнання або продукцію, яку виробляє підприємство.

7. *Атака та відмова в обслуговуванні*. Цілеспрямовані та розподілені атаки можуть зробити систему IIoT недоступною, що, у свою чергу, призведе до зупинення виробництва.

4.10.3. Комплексний підхід щодо захисту систем IIoT

Щоб захистити системи IIoT, необхідно застосовувати комплексний підхід, що передбачає такі заходи:

1. Zero Trust. Прийняття архітектури нульової довіри на підприємстві є стратегічним кроком для підвищення безпеки систем IIoT. Цей підхід ґрунтується на фундаментальному принципі того, що нікому не можна довіряти та все треба перевіряти. Доступ надається виключно за принципом «необхідність знати», що значно знижує ризик несанкціонованого входу та потенційних кіберзагроз.

2. Audit. Усунення ризиків кібербезпеки в системі IIoT вимагає чіткого плану, починаючи з детальної оцінки ризиків. Оцінка ризику допомагає зрозуміти, що може піти не так, наскільки ймовірно це станеться та які наслідки будуть, якщо це станеться. У ньому розглядаються пристрої, датчики, контролери, пункти керування та способи їхньої взаємодії. Після визначення та ранжування ризиків необхідно розробити план заходів для їхнього зменшення.

3. Security Awareness. Наскільки б досконалими не були технічні засоби захисту, останнє слово завжди залишається за людиною. Тому важливо систематично навчати співробітників основам кібербезпеки, прищеплюючи їм звичку використовувати складні паролі, двофакторну аутентифікацію та інші ефективні методи захисту.

4. Update. Для забезпечення кібербезпеки систем IIoT протягом усього їхнього життєвого циклу необхідно розробити ефективні процеси автоматичного оновлення. Це особливо важливо в умовах, коли кількість пристроїв у мережі постійно зростає. Підприємства мають віддавати пріоритет структурованим процесам оновлення, вибираючи системи, які підтримують автоматичні оновлення та мають тривалий термін експлуатації.

5. LAN Segmentation. Відокремлення мереж для підключених машин від загальних офісних або гостьових мереж має важливе значення для підвищення безпеки. Доступ до цих спеціалізованих мереж необхідно суворо контролювати, а облікові дані надавати лише необхідному персоналу, щоб запобігти несанкціонованому доступу та потенційним порушенням безпеки.

6. Access Management. Контроль доступу, аутентифікація та шифрування є основними для захисту каналів мережевого зв'язку. Не підлягає обговоренню гарантія безпеки всіх комунікацій, включаючи передання даних і віддалений доступ між пристроями IIoT та системами керування. Крок за кроком мережа захищається від несанкціонованого проникнення, а цілісність даних, що передаються, зберігається. Впровадження та використання систем Privileged Access Management (PAM) та Secure Remote Access (SRA) можна вважати обов'язковим для підприємств із IIoT.

7. Unified cybersecurity management. Централізація управління кібербезпекою має важливе значення для підвищення рівня захисту в IT-мережі організації та мережі систем IIoT. Уніфікована платформа моніторингу та керування дозволяє підрозділу кібербезпеки спостерігати за всіма процесами та швидко впроваджувати засоби контролю й політики в IC.

8. Використання методів апаратного захисту: Physically Unclonable Function (PUF), Trusted Platform Module (TRM) та Hardware Security Module (HSM). Кожен із методів може бути використаний як окремо, так і в поєднанні з іншими. Поєднання методів PUF, TRM та HSM в одній системі IIoT створює багаторівневий захист даних. Кожен із цих методів виконує свою унікальну роль, доповнюючи один одного й забезпечуючи високий рівень кібербезпеки.

Загальна архітектура захисту системи IIoT, що поєднує всі три методи, має бути така:

1. На базовому рівні знаходиться PUF, якій генерує унікальний цифровий відбиток, заснований на фізичних характеристиках пристрою.

Цей відбиток неможливо точно відтворити, що робить його ідеальним для аутентифікації пристрою в системі IIoT. PUF може використовуватися для зберігання частини ключа шифрування, що робить його більш стійким до атак.

2. На середньому рівні знаходиться TRM, завданням якого є перевірка цілісності системи IIoT. TRM постійно моніторить її стан, перевіряючи, чи не було внесено зміни до програмного або апаратного забезпечення. TRM може генерувати криптографічні ключі для шифрування даних та аутентифікації, які зберігає в безпечному середовищі, захищаючи від несанкціонованого доступу.

3. На верхньому рівні знаходиться HSM. Це спеціалізовані пристрої, призначені для захисту криптографічних ключів і конфіденційних даних, запобігаючи несанкціонованому доступу та підробці. Їх інтеграція в інфраструктуру безпеки знижує ризик компрометації даних. HSM виконує складні криптографічні операції, такі як шифрування, дешифрування та підпис цифрових документів. Він захищений від фізичних атак і має вбудовані механізми захисту від програмних атак.

Взаємодія методів PUF, TRM та HSM відбувається таким чином:

PUF та TRM. PUF забезпечує унікальний ідентифікатор пристрою, який використовується TRM для перевірки цілісності системи. TRM може також використовувати PUF для генерації частини ключа, що зберігається в HSM.

TRM та HSM. TRM генерує ключі, які передаються в HSM для зберігання. HSM виконує криптографічні операції з використанням цих ключів.

Таким чином, поєднання трьох методів апаратного захисту (PUF, TRM, HSM) створює потужну і гнучку багаторівневу архітектуру для захисту даних. Кожен із цих методів виконує свою унікальну роль, доповнюючи один одного й забезпечуючи високий рівень кібербезпеки. Наведена архітектура може бути використана в різних галузях, де висуваються високі вимоги до кібербезпеки.

Отже, системи промислового Інтернету речей стають дедалі більш поширеними, але водночас і більш вразливими до кібератак. Захист систем IIoT є досить складним завданням, яке вимагає комплексного підходу. Промислові та інфраструктурні підприємства й організації мають інвестувати в безпеку своїх систем IIoT та за допомогою розглянутих засобів і методів покращувати їхній захист, щоб уникнути серйозних наслідків кібератак.

Висновки до четвертого розділу

На сьогоднішній день серед вітчизняних організацій можна виділити такі підходи до забезпечення інформаційної та кібербезпеки: ситуаційний, інтеграційний та інтеграційно-інноваційний. Розглянувши ці підходи, можна зробити висновок, що інформаційна та кібербезпека має ґрунтуватися на комплексному підході та ефективній інтеграції всіх елементів ІТ-інфраструктури на різних рівнях їхньої взаємодії. Це зумовлено впровадженням нових методів організації роботи в організаціях, передових ІТ-технологій, повсюдної автоматизації та цифровізації, розповсюдженням хмарних технологій, BYOD, SD-WAN, IoT.

Протидіяти різноманітним видам сучасних кібератак і кіберзагроз можна, лише підвищуючи рівень кіберзахисту ІС, який можна поділити на дві основні складові: технічну та організаційну. Технічна складова є більш об'ємною й містить сукупність технічних засобів – апаратно-програмних та програмних, які захищають ІС в цілому та її окремі елементи від несанкціонованих дій користувачів та зовнішніх зловмисників. Організаційна складова описує, яким чином, відповідно до яких керівних та статутних документів, за допомогою яких технічних рішень, які спеціалісти будуть захищати ІС та від яких саме загроз. Організаційна складова – це побудована ієрархічна система документів від загального – концепція кібербезпеки до конкретного – політики та інструкції на всі випадки порушення кібербезпеки, які можуть статись з ІС в цілому та окремими конкретними її елементами. Вона базується на нормах національного законодавства та міжнародних і національних стандартах захисту ІС та інформації. Поєднання організаційної та технічної складових разом створює комплексний підхід до захисту ІС від різноманітних кіберзагроз. Ефективний захист ІС будь-якої організації потребує такого комплексного підходу та постійного вдосконалення.

Важливим для безпеки організації є захист корпоративних БД та інформації в них. Захист інформації – це основне завдання процесу управління БД, що містить такі компоненти: фізичний захист БД; захист продуктивності БД та їх моніторинг; захист даних у БД від знищення чи пошкодження; контроль доступу; облік нових БД, що з'являються в інфраструктурі. Найбільш дієвим засобом захисту БД є впровадження спеціалізованих програмно-апаратних комплексів, розроблених для захисту БД, захисту вебдодатків, очищення нелегітимного трафіку, захисту від використання вразливостей, зокрема Imperva DBS та Imperva WAF. Застосування Imperva DBS допоможе вирішити всі ключові завдання захи-

сту БД та забезпечить повну видимість та контроль використання БД в інфраструктурі організації.

Тести на проникнення – це процеси, спрямовані на виявлення слабких місць в ІС, додатках або мережах шляхом симуляції реальних атак. Основою цього процесу стає активний аналіз ІС із виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних або технічних контрзаходах. Існує багато різновидів тестів на проникнення. Найбільш поширені – ті, що класифікуються за типом доступу до інформації, що надається тестерам, та за основним об'єктом тестування. Зазначимо, що обидва можна й треба використовувати в комбінації, бо, за деякими винятками, кожен із тестів на проникнення буде відповідати одному з типів з обох класифікацій. Отже, тестування на проникнення є одним з основних типів оцінювання рівня кібербезпеки ІС та засобом його підвищення. Сьогодні розвиток напрямку тестування на проникнення поєднує тренди на подальшу автоматизацію, використання хмарних інструментів, штучного інтелекту в аналізі вразливостей, збільшення ролі тестів, що використовують соціальну інженерію.

Керування вразливостями – це організаційно-технічний процес і набір практик для виявлення, оцінки, пріоритизації, усунення (або пом'якшення) і валідації вразливостей у програмному та апаратному забезпеченні в ІТ-системах та системах промислової автоматизації, які використовують державні та комерційні установи. Під уразливістю розуміється помилка або слабкість у дизайні, реалізації чи управлінні інформаційної системи, яку може експлуатувати зловмисник і яка може призвести до порушення конфіденційності, цілісності або доступності системи.

Керування вразливостями – це організаційно-технічний проактивний процес і набір практик для виявлення, оцінки, пріоритизації, усунення й валідації вразливостей у програмному та апаратному забезпеченні в ІТ-системах та системах промислової автоматизації, який забезпечує захист ІС та мереж від кібератак і порушень безпеки даних. Тож це важлива частина загальної програми гарантування безпеки. Визначаючи, оцінюючи й ліквідуючи потенційно слабкі місця в системі безпеки, організації можуть запобігти атакам і, якщо вони все ж трапляться, мінімізувати збитки. Мета керування вразливостями полягає в тому, щоб знизити загальну схильність організації до ризиків, усуваючи якомога більше вразливостей. Керування вразливостями має бути безперервним процесом відстеження нових загроз і змін середовища.

Безпечне розроблення ПЗ – це підхід, який включає аспекти безпеки на всіх етапах життєвого циклу розроблення. Його мета полягає в тому, щоби забезпечити створення ПЗ, стійкого до кібератак. Основні етапи безпечного розроблення охоплюють: аналіз вимог, проєктування, розроблення, тестування, розгортання, технічну підтримку та обслуговування. А ключовими принципами безпечного розроблення ПЗ є превентивні заходи, мінімізація ризиків на ранніх етапах, безперервна інтеграція безпеки, а також навчання та свідомість команди розробників щодо питань безпеки.

Зміна процесів роботи в корпоративних ІС показала актуальність і необхідність посилення заходів для забезпечення інформаційної та кібербезпеки при застосуванні віддаленого доступу для можливості розподіленої роботи співробітників і забезпечення вільного переміщення інформації в корпоративній мережі з високою швидкістю її поширення. Але ці зміни несуть і нові загрози: ослаблення контролю доступу до інформації, її неконтрольоване поширення, складність оцінки важливості інформації в динамічно мінливих умовах. Ефективно протистояти виниклим загрозам можна, використовуючи системи мультифакторної аутентифікації та шифрування, DLP, MDM, PAM і системи відеоконференцій. У цьому випадку комунікація між користувачами корпоративної ІС мережі буде швидкою й захищеною.

Проведений аналіз проблеми використання IoT-пристроїв як дуже простого й масового способу зараження вірусами ІС підтверджує необхідність організації ефективної протидії цьому виду кіберзагроз. Розроблені рекомендації щодо забезпечення кібербезпеки IoT-пристроїв підтверджують, що такі можливості існують. Однак малоймовірно, що виробники IoT-пристроїв і тим більше оператори зв'язку захочуть самостійно вжити необхідних заходів для їхнього кіберзахисту. З огляду на всю серйозність такого виду кіберзагроз розв'язання регуляторних питань у цій сфері має взяти на себе держава, оскільки для забезпечення кібербезпеки під час масового використання IoT-пристроїв потрібно внести відповідні зміни до національної нормативно-правової бази.

Промисловий Інтернет речей – це концепція, яка поєднує в собі потужність глобальної інформаційної мережі та традиційної промисловості. Вона об'єднує новітні досягнення у сфері інформаційних та виробничих технологій, такі як ШІ, високошвидкісний обмін даними, бездротові технології, обробка великих обсягів інформації в режимі реального часу та багато іншого. Промисловий Інтернет речей, незважаючи на всі свої переваги, стикається з низкою серйозних загроз, які можуть

призвести до порушення виробничих процесів, значних фінансових втрат та навіть фізичної шкоди, тому що саме виробництво є великим об'єктом для кібератак. Системи промислового Інтернету речей стають дедалі більш поширеними, але водночас і більш вразливими до кібератак. Захист систем промислового Інтернету речей є досить складним завданням, яке вимагає комплексного підходу. Отже, поєднання трьох методів апаратного захисту (PUF, TRM, HSM) створює потужну і гнучку багаторівневу архітектуру для захисту даних. Кожен із цих методів виконує свою унікальну роль, доповнюючи один одного й забезпечуючи високий рівень кібербезпеки. Така архітектура може бути використана в різних галузях, де висуваються високі вимоги до кібербезпеки, щоб уникнути серйозних наслідків кібератак.

Перелік використаних джерел:

1. Лисецький Ю. М., Калбазов Д. Й. Підходи до забезпечення інформаційної безпеки підприємств. Математичні машини і системи. 2023. № 4. С. 26–32.
2. What is a Security Operations Center (SOC)? URL: https://www.ibm.com/topics/security-operations-center (дата звернення: 10.03.2023).
3. Лисецький Ю. Центр реагування на інциденти інформаційної безпеки. Матеріали науково-практичної конференції «Сектор безпеки і оборони України: технології асиметричного протиборства» 04.12.2020. № 42. С. 22.
4. Бобров С., Лисецький Ю. Security Operation Systems. Математичні машини і системи. 2020. № 2. С. 51–59.
5. Тернавский В., Калбазов Д., Лисецький Ю. Система моніторингу та автоматизації обробки інцидентів. Математичні машини і системи. 2020. № 3. С. 80–86.
6. Business Continuity Plan | Kyndryl. URL: https://www.kyndryl.com/nz/en/learn/plan (дата звернення: 10.03.2023).
7. IT Disaster Recovery Plan – Ready.gov. URL: https://www.ready.gov/it-disaster-recovery-plan (дата звернення: 12.03.2023).
8. BYOD-стратегии, ориентированные на сотрудников. URL: http://allta.com.ua/about-byod (дата звернення: 12.03.2023).
9. Next Generation Firewall (NGFW) проти кібератак. URL: https://hub.kyivstar.ua/news/next-generation-firewall-nadijnyj-shhyt-vid-novyh-kiberatak-na-biznes/ (дата звернення: 16.03.2023).

10. SIEM (Security information and event management). URL: https://it-guild.com/info/glossary/siem/ (дата звернення: 18.03.2023).

11. Рівні моделі OSI. URL: http://smartandyoung.com.ua/rivni-modeli-osi (дата звернення: 20.03.2023).

12. DNS – что это и как работает. URL: https://hostiq.ua/blog/ukr/how-does-dns-work/ (дата звернення: 24.03.2023).

13. Что такое SD-WAN – сложная технология простыми словами. URL: https://gigatrans.ua/ru/news/chto-takoe-sd-wan-slozhnaya-tehnologiya-prostumi-slovami (дата звернення: 24.03.2023).

14. What is a Cloud Access Security Broker (CASB)? URL: https://www.wiz.io/academy/what-is-a-cloud-access-security-broker-casb (дата звернення: 28.03.2023).

15. AWS Identity and Access Management (IAM) – Explained With. URL: https://www.freecodecamp.org/news/aws-iam-explained/ (дата звернення: 10.03.2023).

16. WAF (Web Application Firewall) – межсетевой экран для веб-приложений. URL: https://itglobal.com/ru-ru/company/glossary/waf/ (дата звернення: 28.03.2023).

17. The Advanced Persistent Threat (or Informagonized Force Operagons). Michael K. Daly. November 4, 2009. URL: https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf (дата звернення: 26.06.2024).

18. Assessing Outbound Traffic to Uncover Advanced Persistent Threat. URL: https://www.researchgate.net/publication/333634056_Assessing_Outbound_Traffic_to_Uncover_Advanced_Persistent_Threat (дата звернення: 26.06.2024).

19. FireEye Advanced Threat Protection – What You Need to Know. URL: https://www.slideshare.net/slideshow/fireeye-advanced-threat-protection-what-you-must-know/14655845 (дата звернення: 26.06.2024).

20. Основи кібербезпеки. URL: https://gurt.org.ua/news/informator/41918/ (дата звернення: 26.06.2024).

21. Організаційно-технічна модель кіберзахисту. URL: https://cip.gov.ua/ua/news/organizaciino-tekhnichna-model-kiberzakhistu (дата звернення: 26.06.2024).

22. Лисецький Ю. М., Данченко О. І. Організаційні методи підвищення рівня кіберзахисту. Вісник воєнної розвідки. 2025. № 87. С. 41–45.

23. Total data volume worldwide 2010-2025 – Statista/ URL: https://www.statista.com/statistics/871513/worldwide-data-created/ (дата звернення: 17.02.2023).

24. Лисецький Ю. М., Козаченко С. В. Програмно-визначені системи зберігання даних. Переваги і особливості. Математичні машини і системи. 2021. № 1. С. 17–23.

25. Лисецький Ю. М. Захист баз даних. Modern research in science and education: зб. тез III міжнарод. наук.-практ. конф. (м. Чикаго, США, 9–11 листопада 2023 р.). Чикаго, 2023. С. 277–280.

26. Лисецький Ю. М., Калбазов Д. Й. Інформаційна безпека корпоративних баз даних. Математичні машини і системи. 2023. № 3. С. 31–37.

27. Что такое SQL-инъекции и как им противостоять. URL: https://highload.today/sql-inektsii/ (дата звернення: 18.02.2023).

28. What is a Stored Procedure? – Definition from WhatIs.com. URL: https://www.techtarget.com/searchoracle/definition/stored-procedure#:~:text=A%20stored%20procedure%20is%20a,and%20shared%20by%20multiple%20programs (дата звернення: 18.02.2023).

29. The Model View Controller Pattern – MVC Architecture and Frameworks Explained. URL: https://www.freecodecamp.org/news/the-model-view-controller-pattern-mvc-architecture-and-frameworks-explained/ (дата звернення: 19.02.2023).

30. Imperva Database Security. URL: https://www.imperva.com/resources/datasheets/Imperva-Database-Security-Datasheet-2020.pdf (дата звернення: 19.02.2023).

31. Лисецкий Ю. М. Информационная безопасность: защита от DDoS-атак. Сборник тезисов международной научно-практической конференции «Системный анализ и информационные технологии», 26-30 июня, НТУ «КПИ». С. 405–406.

32. Intrusion Detection Systems: A Modern Investigation. URL: https://www.academia.edu/13787335/Intrusion_Detection_Systems_A_Modern_Investigation (дата звернення: 20.02.2023).

33. Imperva Web Application Firewall (WAF) | App & API Protection. URL: https://www.imperva.com/products/web-application-firewall-waf/ (дата звернення: 20.02.2023).

34. Penetration Testing History. Retrieved. URL: https://christianespinosa.com/blog/penetration-testing-history/ (дата звернення: 12.12.2024).

35. Bacudio, A., Yuan, X, Chu, B., Jones, M. (2011). An Overview of Penetration Testing. International Journal of Network Security & Its Applications. 3. 19-38. 10.5121/ijnsa.2011.3602. (дата звернення: 16.12.2024).

36. Лисецький Ю. М., Старовойтенко О. О. Тестування на проникнення як засіб підвищення рівня кібербезпеки інформаційних систем. Математичні машини і системи. 2025. № 2. С. 24–29.

37. Тести на проникнення. Retrieved on 12.12.2024. URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F (дата звернення: 12.12.2024).

38. Alhamed, M. & Rahman, M. (2022). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. Applied Sciences, 13(12), 6986. URL: https://doi.org/10.3390/app13126986 (дата звернення: 22.12.2024).

39. Ferdous, R. & Suchi, U. (2024). Evaluating Penetration Testing and Methodologies. URL: https://www.researchgate.net/publication/382617676_Evaluating_Penetration_Testing_and_Methodologis (дата звернення: 22.12.2024).

40. Software Testing – White Box Penetration Testing (2024). URL: https://www.geeksforgeeks.org/software-testing-white-box-penetration-testing/ (дата звернення: 02.01.2025).

41. Altulaihan, E., Alismail, A., & Frikha, M. (2022). A Survey on Web Application Penetration Testing. Electronics, 12(5), 1229. URL: https://doi.org/10.3390/electronics12051229 (дата звернення: 02.01.2025).

42. Makadia, H. & Kotadia, J. (2021). Mobile Security and Penetration Testing. International Journal of Advanced Research in Science, Communication and Technology. PP. 455-460. 10.48175/IJARSCT-2215.

43. Network Penetration Testing (2024). URL: https://www.blackduck.com/glossary/what-is-network-penetration-testing.html (дата звернення: 04.01.2025).

44. Соціальна інженерія: що це та як уберегтися від шахрайства (2024). URL: https://www.zen.com/uk/blog/personal-finance-uk/social-engineering-how-to-protect-yourself-from-fraud/ (дата звернення: 02.01.2025).

45. Physical pen testing methods and tools (2023). URL: https://www.techtarget.com/searchsecurity/tip/Physical-pen-testing-methods-and-tools (дата звернення: 08.01.2025).

46. Лисецький Ю. М. Підвищення ефективності тестування інформаційних систем на проникнення за допомогою штучного інтелекту. Вісник воєнної розвідки. 2025. Спецвипуск «Штучний інтелект у сфері безпеки і оборони». С. 81–85.

47. Holm, H., Sommestad, T., Almroth, J., & Persson, M. (2011). A quantitative evaluation of vulnerability scanning. Information Management & Computer Security. 2011. 19 (4). PP. 231–247.

48. Nessus Official | Vulnerability Management Tools. URL: https://www.tenable.com/blog/nessus-turns-15 (дата звернення: 07.04.2025).

49. Karlsson, Mathias. The Edit History of the National Vulnerability Database and similar Vulnerability Databases. 2012. P. 101.

50. CISA KEV — A Balanced Perspective. URL: https://medium.com/@yotamperkal/cisa-kev-a-balanced-perspective-ff3856e69ba9 (дата звернення: 07.04.2025).

51. Brumă O.-V. (2020). Vulnerabilities of Information Systems. International Journal of Information Security and Cybercrime. 2020. 9 (1). PP. 9–14.

52. Mell P, Spring J (2025) Likely Exploited Vulnerabilities: A Proposed Metric for Vulnerability Exploitation Probability. National Institute of Standards and Technology, Gaithersburg, MD. 2025. P. 30.

53. Souppaya M., Scarfone K. NIST Special Publication 800-40 Revision 4: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. URL: https://csrc.nist.gov/pubs/sp/800/40/r4/final (дата звернення: 07.04.2025).

54. Bennouk K., Ait Aali N., El Bouzekri El Idrissi, Sebai B., Faroukhi A. Z., Mahouachi D. A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies. Journal of Cybersecurity and Privacy. 2024. 4 (4). PP. 853–908.

55. CVE: Common Vulnerabilities and Exposures. URL: https://www.cve.org/about/history (дата звернення: 07.04.2025).

56. Li Z., Sun L., Xu W., Chi C. H., Xue Y. Vulnerability scanning and analysis in large-scale heterogeneous systems. Journal of Computer Security. 2021. 29 (2). PP. 135–162.

57. Shu R., Gu X., Enck W. A study of security vulnerabilities on Docker Hub. Proceedings of the Seventh ACM Conference on Data and Application Security and Privacy. 2017. PP. 269–280.

58. Khan R., McLaughlin K., Laverty D., Sezer S. STRIDE-based threat modeling for cyber-physical systems. 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). 2020. PP. 1–6.

59. Fruhlinger, J. What is vulnerability management? A process for securing software and networks. CSO Online. 2019. PP. 27–32.

60. Doupe A., Cova M., Vigna G. Why Johnny can't pentest: An analysis of black-box web vulnerability scanners. Detection of Intrusions

and Malware, and Vulnerability Assessment (DIMVA 2010). 2010. PP. 111–131.

61. Mell P., Scarfone K., Romanosky S. A complete guide to the Common Vulnerability Scoring System version 2.0. URL: https://www.nist.gov/publications/complete-guide-common-vulnerability-scoring-system-version-20 (дата звернення: 07.04.2025).

62. Jacobs J., Spring J., Stoner E., Sauerwein C. Exploit Prediction Scoring System (EPSS). Proceedings of the 2021 IEEE European Symposium on Security and Privacy Workshops. 2021. PP. 587–596.

63. Sabottke C., Suciu O., Dumitraş T. Vulnerability disclosure in the age of social media: Exploiting Twitter for predicting real-world exploits. 24th USENIX Security Symposium (USENIX Security 15). (2015). PP. 1041–1056.

64. Scarfone K., Mell P. Guide to vulnerability scanning tools. NIST Special Publication 800-115. National Institute of Standards and Technology. 2007. P. 79.

65. Gupta S., Badve O., Vora P. Automated vulnerability assessment and penetration testing using Nessus. International Journal of Computer Applications. 2020. 176 (38). PP. 1–7.

66. Fang Z., Zhang L., Chen Y., Chen Z. Research on vulnerability detection technology in software security. IEEE Access. 2020. 8. PP. 197586–197600.

67. Shu R., Gu X., Enck W. A study of security vulnerabilities on Docker Hub. Proceedings of the Seventh ACM Conference on Data and Application Security and Privacy. 2017. PP. 269–280.

68. Li Z., Sun L., Xu W., Chi C. H., Xue Y. Vulnerability scanning and analysis in large-scale heterogeneous systems. Journal of Computer Security. 2021. 29 (2). PP. 135–162.

69. Zhang Y., Chen X., Xiang Y. Context-aware risk-based vulnerability management. Future Generation Computer Systems. (2019). 94. PP. 444–456.

70. Jacobs J., Spring J., Stoner E., Sauerwein C. Exploit Prediction Scoring System (EPSS). Proceedings of the 2021 IEEE European Symposium on Security and Privacy Workshops. 2021. PP. 587–596.

71. Rahman M. S., Williams L., Bradshaw G. A framework for improving security patch management in DevOps. Proceedings of the 2019 International Conference on Software and System Processes. 2019. PP. 134–143.

72. DevSecOps: Інтеграція безпеки продукту на кожному етапі SDLC. URL: https://cloudfresh.com/ua/cloud-blog/devsecops-intehratsiya-produktu-bezpeky-na-kozhnomu-etapi-sdlc/ (дата звернення: 12.02.2024).

73. Лисецький Ю. М., Старовойтенко О. О. Безпечна розробка програмного забезпечення. Social ways of training specialists in the social sphere and inclusive education: зб. ст. XIII Міжнародної науково-практичної конференції (м. Прага, Чехія, 01–03 квітня 2024 р.). С. 339–343.

74. Лисецький Ю. М. Інформаційні технології в управлінні та обробці інформації : монографія. Київ : ЛАТ&К, 2018. 268 с.

75. Лисецький Ю. М., Калбазов Д. Й. Особливості управління правами користувачів у корпоративних ІТ системах. Математичні машини і системи. 2023. № 2. С. 28–33.

76. Service Desk: что это и как помогает бизнесу. URL: https://it-guild.com/info/blog/service-desk-chto-eto-i-kak-pomogaet-biznesu/ (дата звернення: 07.01.2023).

77. Лисецький Ю. М. Управління доступом до ІТ-систем. Scientists and existing problems of human development: матеріали IX Міжнародної науково-практичної конференції (м. Загреб, Хорватія, 14–17 листопада 2023 р.). С. 378–379.

78. Лисецький Ю. М. Забезпечення інформаційної безпеки в корпоративній мережі при віддаленому доступі. Інформаційні системи та технології. Стан і перспективи: монографія / Бармак О., Божаткін С. та ін.; під наук. ред. проф. В. Вичужаніна. – Одеса : НУ «ОМА», 2021. 206 с.

79. ESET Secure Authentication. URL: https://help.eset.com/esa/27/ru-RU/supported_environments.html (дата звернення: 14.08.2024).

80. One Identity. URL: https://www.oneidentity.com/ (дата звернення: 14.08.2024).

81. Что такое DLP-системы, кому и когда они нужны. URL: https://rt-solar.ru/products/solar_dozor/blog/2080/ (дата звернення: 14.08.2024).

82. Что такое MDM-системы и зачем компаниям управлять техникой сотрудников. URL: https://vc.ru/macaroon/185491-chto-takoe-mdm-sistemy-i-zachem-kompaniyam-upravlyat-tehnikoy-sotrudnikov (дата звернення: 14.08.2024).

83. Что такое PAM. URL: https://www.dmosk.ru/terminus.php?object=pam (дата звернення: 14.08.2024).

84. Лисецький Ю. М. Особливості забезпечення інформаційної безпеки при віддаленій роботі в мережі. Інформаційні і управляючі системи і технології: матеріали X міжнарод. наук.-практ. конф. (м. Одеса, 23–25 вересня 2021 р.). Одеса, 2021, С. 58–62.

85. Лисецький Ю. М., Калбазов Д. Й. Технологія Internet of Things. Математичні машини і системи. 2019. № 2. С. 43–50.

86. Лисецький Ю. М., Данченко О. І. Аналіз проблем забезпечення кібербезпеки при використання технології «Інтернету речей». Вісник воєнної розвідки. 2024. № 82. С. 46–50.

87. Лисецький Ю. М., Бобров С. І. Нові загрози інформаційній безпеці, або зброя масового зараження. Математичні машини і системи. 2018. № 1. С. 41–50.

88. Opirskyy I., Holovchak R., Moisiichuk I., Balianda T., Haraniuk S. ПРОБЛЕМИ ТА ЗАГРОЗИ БЕЗПЕЦІ IoT ПРИСТРОЇВ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2021. №3 (11). С. 31–42.

89. Lu Y. and Xu L. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics, in Internet of Things Journal. 2019, Vol. 6, No. 2. P. 2103–2115.

90. Rahman F., Farmani M., Tehranipoor M., Jin Y., Hardware-Assisted Cybersecurity for IoT Devices, 2017 18th International Workshop on Microprocessor and SOC Test and Verification (MTV), Austin, TX, USA, 2017. P. 51–56.

91. Boyes, Hugh; Hallaq, Bil; Cunningham, Joe; Watson, Tim. The industrial internet of things (IIoT): An analysis framework. Computers in Industry. Volume 101, October 2018, Pages 1–12.

92. Лисецький Ю. М. Глобальна мережа малої потужності для Інтернету речей. Information Control Systems and Technologies: Materials of the VII International scientific-practical conference. (Odesa, 17–18 Sept, 2018) Odesa, National Polytechnic University, 2018. pp. 96–98.

93. Industrial Internet of Things (IIoT). URL: https://www.incom-tech.com.ua/iiot (дата звернення: 15.03.2025).

РОЗДІЛ 5
ТЕХНОЛОГІЇ, СИСТЕМИ Й ЗАСОБИ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

5.1. Аналіз можливостей використання перспективних технологій у кібербезпеці

5.1.1. Штучний інтелект

Ідеї створення ШІ виникли в середині XX ст. Алан Тюрінг – один із найвідоміших англійських математиків, логіків і криптографів – був першим, хто здійснив істотні дослідження в галузі, яку він називав «машинним інтелектом» (англ. Machine Intelligence) [1]. 1950 року Тюрінг опублікував статтю «Computing Machinery and Intelligence», у якій запропонував експеримент «Тюрінга» як критерій інтелектуальної поведінки машин [2].

Офіційно термін «штучний інтелект» уведено 1956 року на конференції в Дартмутському коледжі, де група вчених, зокрема Джон Маккарті та Марвін Мінський, обговорювали потенціал створення машин, здатних виконувати завдання, які потребують людського інтелекту.

Практичні кроки у створенні ШІ було зроблено в середині XX ст., коли з'явилися перші комп'ютери. Учені та інженери почали замислюватися над тим, як зробити комп'ютери розумнішими та здатними до автономного прийняття рішень [3–5].

Першим етапом були досягнення в галузі логічного інтелекту. Було створено ПЗ, здатне розв'язувати складні логічні задачі та робити логічні висновки. Наступним етапом стало створення експертних систем – програмних систем, здатних приймати складні рішення в певній сфері на основі знань, накопичених спеціалістами в цій галузі. Ці системи дали можливість автоматизувати вирішення багатьох завдань, що привело до суттєвого збільшення продуктивності та ефективності в різних сферах діяльності.

Наприкінці XX ст. та на початку XXI ст. спостерігався стрімкий розвиток у галузі ШІ. Розвиток комп'ютерів, великих даних та машинного навчання сприяв створенню систем, здатних розпізнавати образи, обробляти природну мову та прогнозувати майбутні події. Ці нові технології застосовуються в багатьох сферах, зокрема в інформаційній та кібербезпеці [6–11].

З огляду на величезні обсяги даних, з якими доводиться працювати на сьогодні, і брак досвідчених фахівців із кібербезпеки переважна більшість організацій уже використовує можливості ШІ для забезпечення кібербезпеки або планує це в майбутньому. Передбачається, що ШІ, узявши на себе більшу частину рутинних процедур, звільнить фахівців від простих і складних завдань [12]. Так, наприклад, ШІ може аналізувати події у сфері кібербезпеки, виявляти відхилення від норми в роботі програм та пристроїв і сповіщати про це співробітників служби кібербезпеки [13, 14].

За оцінкою MarketsandMarkets, у 2019–2026 рр. ринок засобів ШІ для забезпечення кібербезпеки зростатиме в середньому на 23,3 % за рік, з 8,8 до 38,2 млрд доларів (рис. 5.1).

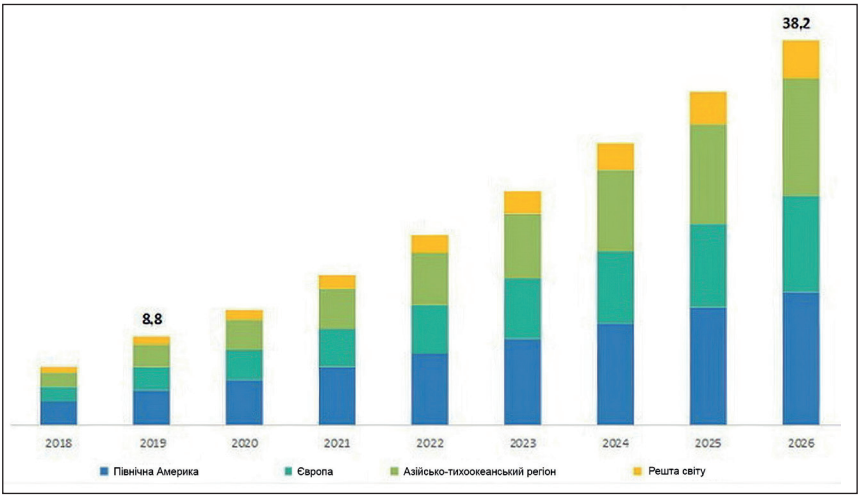

Рис. 5.1. Динаміка зростання ринку засобів ШІ для забезпечення кібербезпеки в регіонах, млрд дол.

ШІ активно використовується для вирішення питань кібербезпеки на багатьох рівнях. Сучасні системи ШІ здатні аналізувати величезні обсяги даних швидше, ніж людина, і виявляти складні шаблони або аномалії, які можуть указувати на потенційні загрози. ШІ застосовується також для підвищення ефективності захисту кінцевих точок, таких як антивіруси та фаєрволи, що дає можливість передбачати і блокувати їх атаки заздалегідь. Основні напрями застосування ШІ у сфері кібербезпеки:

прогнозування загроз (ідентифікація потенційних нових уразливостей та кібератак до того, як вони стануть серйозними проблемами);

автоматизація відповідей на інциденти (реагування ШІ на інциденти безпеки, що скорочує час на їх вирішення);

розумний моніторинг мережі (моніторинг мережевої активності та виявлення аномалій, які можуть свідчити про несанкціонований доступ чи вторгнення);

управління ідентифікацією та доступом (зміцнення систем управління забезпечує можливість доступу тільки уповноваженим користувачам);

шифрування SSL/TLS (безпечні протоколи зв'язку, що використовують ШІ, допомагають забезпечити захист даних під час передання. Зараз ШІ є не просто зручним інструментом, а необхідною складовою системи ефективного захисту від кіберзагроз).

ШІ відіграє ключову роль у прогнозуванні кіберзагроз завдяки своїм спроможностям обробляти великі обсяги даних та виявляти складні зразки поведінки, що зазвичай неможливо в разі застосування традиційних аналітичних методів [15]. У цьому процесі ШІ може допомогти, виконуючи такі функції:

аналіз даних у реальному часі (моніторинг та аналіз мережевого трафіку щодо аномальних поведінок, які вказують на потенційні кіберзагрози);

автоматизація виявлення загроз (автоматизація процесів виявлення та класифікації загроз, що скорочує час реакції на інциденти безпеки);

підвищення точності прогнозів (завдяки машинному навчанню системи на базі ШІ можуть «навчатися» вдосконалюватися через атаки та прогнозувати майбутні загрози);

виявлення невідомих загроз (допомога в ідентифікації нових кіберзагроз, аналізуючи моделі поведінки, що мають відхилення від норми);

адаптація до нових загроз (здатність адаптуватися до змін у кіберзагрозах, постійно оновлюючи бази даних і методи захисту).

Використання ШІ не лише допомагає у прогнозуванні та виявленні кіберзагроз, а й сприяє забезпеченню більш адекватної та ефективної відповіді на кіберінциденти, зменшенню фальшивих спрацьовувань і зниженню витрат на захист ІС.

ШІ може допомогти у вирішенні таких питань:

швидке виявлення інцидентів (аналіз величезних обсягів даних у реальному часі та швидке виявлення аномалій, що вказують на потенційні кібератаки. Це дає можливість своєчасно реагувати на кіберзагрози);

класифікація і пріоритизація інцидентів (допома визначення ступеня небезпеки кіберінцидентів та пріоритизація відповіді з метою зосередження команди кібербезпеки на найкритичніших загрозах);

автоматизоване реагування (на відомі типи атак ШІ може автоматично відповідати такими діями, як ізоляція заражених ІС, блокування зловмисного трафіку або скидання паролів задля мінімізації потенційних збитків);

адаптивне навчання (використовуючи машинне навчання, системи ШІ постійно вдосконалюються на прикладах із кожного кіберінциденту, підвищуючи свою здатність передбачати майбутні кіберзагрози та реагувати на них);

підтримка прийняття рішень (надання рекомендацій щодо оптимальних дій для відповіді на конкретні типи кіберзагроз, допомога аналітикам у прийнятті обґрунтованих рішень із питань кібербезпеки);

зменшення фальшивих спрацьовувань (завдяки точному аналізу даних ШІ може розрізняти легітимну діяльність від справжніх кіберзагроз, зменшуючи кількість хибних тривог і підвищуючи продуктивність роботи команд кібербезпеки).

Застосування ШІ в автоматизації відповідей на інциденти кібербезпеки суттєво підвищує здатність організацій ефективно захищатися від кіберзагроз, скорочує час реакції на інциденти та забезпечує високий рівень захисту ІС.

ШІ може поліпшити моніторинг мереж за допомогою автоматизації та підвищення точності аналізу даних. Зазначимо кілька способів використання ШІ для розумного моніторингу мереж:

автоматизація виявлення аномалій (аналіз патернів мережевого трафіку в реальному часі, виявлення аномалій, які вказують на несанкціонований доступ або інші види кібератак. Це дає можливість швидше реагувати на потенційні загрози);

підвищення точності прогнозування (завдяки машинному навчанню ШІ може більш точно прогнозувати потенційні кіберзагрози та аномалії в мережі, зменшуючи кількість хибнопозитивних спрацьовувань);

оптимізація пропускної здатності (аналіз патернів трафіку з метою оптимізації використання ресурсів мережі, підвищення її ефективності та зниження заторів);

ідентифікація та класифікація загроз (автоматична ідентифікація кіберзагроз та класифікація їх за типами на основі аналізу даних, що дає змогу виявляти потенційні ризики для мережі);

автоматизоване відновлення мережі після кіберінцидентів (автоматизація процесів відновлення мережі після кібератак, швидка ізоляція пошкоджених ІС та відновлення їх нормальної роботи);

безперервне навчання та адаптація (системи ШІ постійно «навчаються», збільшуючи обсяг даних, що дає змогу адаптуватися до нових загроз і тактик кібератак).

Використання ШІ для розумного моніторингу мереж забезпечує більш глибокий і точний аналіз даних, допомагаючи виявляти кіберзагрози і відповідати на них більш ефективно та з меншими витратами ресурсів.

ШІ може суттєво вдосконалити ідентифікацію та доступ до ІС за багатьма параметрами, зокрема:

розпізнавання облич (використання біометричних даних для розпізнавання облич та надання доступу до ІС або приміщень);

аналіз поведінки користувачів (застосування алгоритмів машинного навчання для аналізу звичних дій користувачів допомагає ідентифікувати втручання, що можуть свідчити про неавторизований доступ);

автоматичне управління доступом (автоматизація процесів надання чи відкликання доступу, що базується на визначених критеріях, таких як рівень безпеки, час входу та ін.);

виявлення шкідливого ПЗ (виявлення та блокування шкідливого ПЗ, за допомогою якого зловмисники намагаються дістати несанкціонований доступ до ІС);

посилення кіберзахисту (інтеграція ШІ в системи ідентифікації може посилити кіберзахист, оскільки ШІ постійно навчається та адаптується до нових атак);

інтеграція з іншими системами (легка інтеграція ШІ з різними системами управління ідентифікацією та доступом (IAM) підвищує ефективність управління ідентифікацією).

Використання ШІ в системі управління ідентифікацією та доступом може дати організаціям перевагу у швидкості, точності та ефективності захисту своїх ІС.

ШІ може зіграти ключову роль у посиленні безпеки протоколів зв'язку, як-от SSL/TLS, які використовуються для шифрування даних під час їхнього передання через мережу. Він може це зробити кількома способами:

виявлення аномалій (аналіз шаблонів трафіку мережі з метою виявляння відхилень, які вказують на спроби злому системи шифрування або інші кібератаки);

автоматичне оновлення та підтримка (забезпечення актуальності протоколів, автоматизація оновлення криптографічних ключів та сертифікатів безпеки);

машинне навчання для прогнозування (застосування методів машинного навчання для прогнозування та виявлення потенційних зламів до того, як вони стануться, що дає можливість проактивно захищати ІС);

автоматизоване тестування безпеки (складне тестування безпеки протоколів для виявлення слабких місць та вразливостей у шифруванні даних);

підтримка складних систем (підтримання більш складних систем шифрування, які є занадто важкими для ручного управління).

У використанні ШІ для підтримки безпечних протоколів зв'язку ключовим елементом є постійне вдосконалення технологій та адаптація до нових загроз, можливість масштабування, що необхідно для захисту даних у сучасному цифровому світі.

ШІ відкриває нові горизонти у сфері кібербезпеки, але водночас він може створювати і серйозні загрози [16]:

автоматизація атак (використання ШІ для створення і проведення швидких та ефективних кібератак, які важко виявляти та блокувати традиційними методами);

поліпшення фішингових атак (за допомогою ШІ фішингові атаки можуть стати більш переконливими, оскільки здатні імітувати патерни людського письма і поведінки);

використання у глибоких підробках (deepfake) (створення дуже реалістичних аудіо- і відеопідробок, що сприяють поширенню дезінформації та впливу на громадську думку або індивідуальні рішення);

маніпулювання даними (використання ШІ для маніпулювання даними або їх зміна без виявлення, що може мати серйозні наслідки для збереження цілісності інформації);

створення нових видів уразливостей (інтеграція ШІ в системи кібербезпеки може також відкрити нові вразливості, які можуть бути використані зловмисниками);

автономні кіберзброї (використання ШІ у створенні автономної кіберзброї призведе до незворотних атак, які можуть бути запущені без людського втручання.

Отже, ключ до захисту проти цих загроз – розроблення комплексних стратегій кібербезпеки, які передбачають використання ШІ як інструменту захисту. Незважаючи на майбутні перспективи використання ШІ у сфері кібербезпеки, усе ж є обмеження, про які варто

зазначити. Для машинного навчання потрібні набори даних, проте в деяких випадках їх збирання і використання можуть суперечити законам про конфіденційність інформації. Для побудови точних моделей програмних систем, навчальних алгоритмів потрібна велика кількість даних, що погано поєднується з «правом на забуття». Виявлена в деяких даних інформація, за якою ідентифікують людину, може порушувати її права, тому необхідно передбачити можливі рішення цієї проблеми. Одне з них – використання систем, які практично унеможливлюють доступ до вихідних даних після навчання. Анонімізація наборів таких даних також розглядається як можливий метод, що потрібно дослідити глибше, аби уникнути спотворення логіки програм. Для забезпечення кібербезпеки на базі ШІ галузі потрібно більше кваліфікованих експертів. Ефективність засобів мережевої безпеки, основаних на ШІ, стане набагато вище за наявності фахівців, здатних обслуговувати й налаштовувати їх відповідно до потреб.

5.1.2. Квантові технології

Квантові технології відкривають принципово нові можливості як у цивільному, так і військовому застосуванні. Останнім часом ці технології привертають значний інтерес із боку промисловості та урядів [17,18]. Великі технологічні компанії, такі як IBM, Google і Microsoft, витрачають сотні мільйонів доларів на науково-дослідні роботи в галузі квантового обчислення в перегонах за «квантове верховенство». Так само уряди визнали трансформаційний потенціал і геополітичну цінність застосувань квантової технології. США, ЄС і Китай започаткували власні дослідницькі програми вартістю понад мільярд доларів. Зважаючи на потенційні наслідки новітніх квантових технологій для оборони і безпеки, НАТО визначає квантові технології як один із провідних і проривних технологій за впливом на безпеку [19].

Не вдаючись у детальне пояснення квантової механіки, варто звернути увагу на декілька головних основоположних принципів для того, щоб зрозуміти потенціал застосування квантових технологій.

Квантові технології використовують фізичні явища на атомному і субатомному рівні. Основоположним для квантової механіки є те, що на цьому атомному рівні світ є «вірогіднісним» на противагу «детерміністському». Це поняття вірогідності було предметом відомих в усьому світі дискусій між Альбертом Ейнштейном і Нільсом Бором на п'ятому Солвеївському конгресі з фізики в Брюсселі в жовтні 1927 року [20].

Під час дискусій на Солвеївському конгресі 1927 року Нільс Бор захищав нову теорію квантової механіки, сформульовану Вернером Гайзенбергом, у той час як Альберт Ейнштейн намагався підтримувати детерміністську парадигму причини і наслідку. Сьогодні наукова громада вважає, що Нільс Бор переміг у дискусії. Це означає, що наш світ не має розписаного сценарію на основі причини і наслідку, а фактично залежить від випадку.

Нова вірогіднісна парадигма проклала шлях до кращого розуміння деяких головних властивостей квантових часток, які покладено в основу квантових технологій, особливо «суперпозиції» і «зчеплення». Краще розуміння цих фундаментальних квантових принципів стимулювало розвиток квантових технологій нового покоління: квантових сенсорів, квантового зв'язку і квантового обчислення (рис. 5.2).

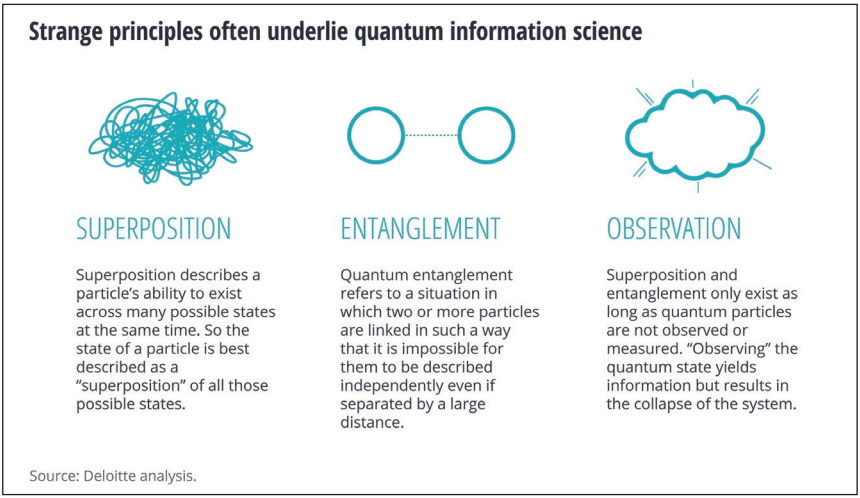

Рис. 5.2. Головні принципи квантової механіки

Квантові технології мають потенціал принести абсолютно нові можливості, дозволити нам відчувати те, що не відчувається, трансформувати кібербезпеку і дати нам змогу розв'язувати проблеми, які ми ніколи раніше не могли розв'язати [21]. У середовищі оборони і безпеки два застосування матимуть особливо значний вплив у найближчій і середній перспективі [22].

По-перше, *квантові сенсори*. Вони ґрунтуються на ультрахолодних атомах або фотонах, якими обережно маніпулюють за допомогою

суперпозиції або зчеплення в конкретних «квантових станах». Використовуючи той факт, що квантові стани надзвичайно чутливі до порушень, квантові сенсори здатні вимірювати дуже малі розбіжності в усіх видах різних властивостей, таких як температура, прискорення, гравітація або час. Квантові сенсори мають потенціал трансформувати нашу технологію вимірювання і виявлення. Вони не лише дозволяють здійснювати набагато точніші й чутливіші вимірювання, але й відкривають можливості для вимірювання речей, які ми ніколи раніше не були здатні виміряти.

Квантові сенсори можуть мати дуже перспективне військове застосування. Наприклад, можуть використовуватися для виявлення субмарин і літаків-невидимок, для високоточної навігації і синхронізації PNT (Position, Navigation, Timing). Такі «квантові пристрої PNT» можуть використовуватись як надійні інерційні навігаційні системи, які забезпечують навігацію без необхідності в зовнішній прив'язці, такій як GPS (Global Positioning System). Це може надати радикально нові можливості, наприклад, для підводної навігації підводних човнів, а також як запасна система навігації для надводних платформ у разі втрати сигналу GPS.

Перші квантові сенсори вже з'явилися на ринку, ставши найбільш розвиненою технологією серед сенсорів, зв'язку та обчислення. Ба більше, у сфері квантового зв'язку й обчислення очікується, що цивільний сектор буде активно їх розвивати, зважаючи на неймовірний потенціал, який вони мають для цивільної промисловості. Проте потенційне застосування квантових сенсорів, таких як квантові PNT і квантовий радар, особливо цікаве для військових. Тому саме військовим потрібно фінансувати, підтримувати і спрямовувати науково-дослідну роботу в цій сфері для того, щоб ці потенційні застосування стали реальністю.

По-друге, *квантовий зв'язок*. Потенціал квантового зв'язку визначається його обіцянкою забезпечити «ультразахищене» передавання даних, потенційно навіть повністю не доступне для хакерів. Нині наш обмін даними залежить від потоків електричних сигналів, що являють собою одиниці (1) і нулі (0), які біжать по оптоволоконних кабелях. Хакер, якому вдається підключитися до такого кабеля, може читати і копіювати ці біти в міру їхнього руху по кабелю. З іншого боку, у квантовому зв'язку інформація, що передається, закодована у квантову частку в суперпозиції 1 і 0, так званий кубіт. Завдяки чутливості квантових станів до зовнішніх подразників щоразу, коли хакер намагається захопити інформацію, що передається, кубіт «згортається» або до 1, або до 0 – таким чином знищуючи квантову інформацію і залишаючи підозрілий слід.

Першим застосуванням квантового зв'язку став так званий квантовий розподіл ключів QKD (Quantum Key Distribution), у якому квантові частки використовуються для обміну криптографічними ключами. В QKD самі дані передаються традиційною інфраструктурою зв'язку, у той час як необхідні для розшифрування даних криптографічні ключі передаються окремо за допомогою квантових часток. Уже ведуться широкомасштабні експерименти з QKD із застосуванням як наземних ліній зв'язку, так і космічного зв'язку. У 2016 році Китай запустив перший у світі квантовий науковий супутник «Міціус», який уже продемонстрував міжконтинентальне QKD «земля-супутник» та «супутник-земля», забезпечивши захищену відеоконференцію між Пекіном і Віднем.

«Квантова телепортація» може стати наступним кроком у квантовому зв'язку. Якщо у QKD криптографічні ключі поширюються із застосуванням квантової технології, при квантовій телепортації сама інформація передається із застосуванням зчеплених квантових пар. Найбільша відстань, на яку досі була здійснена телепортація за допомогою оптоволоконного кабеля, становить 50 кілометрів, і на найближчі роки стоїть завдання розвитку квантової телепортації задля забезпечення захищеного зв'язку на більші відстані.

Кінцевою метою квантового зв'язку є створення «квантового Інтернету»: мережі зчеплених між собою квантових комп'ютерів, підключених до ультразахищеного квантового зв'язку, гарантованого фундаментальними законами фізики. Проте квантовому Інтернету потрібна не лише квантова телепортація на дуже великі відстані, йому також буде потрібний подальший розвиток інших важливих допоміжних технологій, таких як квантові процесори, комплексний квантовий стек Інтернету, який передбачає інтернет-протоколи і програмне забезпечення квантового Інтернету.

По-третє, *квантове обчислення,* яке значно посилить нашу здатність розв'язувати деякі з найскладніших проблем обчислення. У той час як класичні комп'ютери здійснюють обчислення за допомогою бінарних чисел (0 або 1), квантові комп'ютери представляють інформацію, використовуючи квантові біти (кубіти), які можуть бути в суперпозиції обох станів (0 і 1 водночас). Оскільки кубіти надзвичайно чутливі до зовнішніх подразників, то для того щоб контролювати, маніпулювати і використовувати їх, кубіти потрібно охолоджувати до рівня, що наближається до абсолютного мінімуму температури (або нуля по Кельвіну).

Кубіти дозволяють квантовим комп'ютерам робити численні обчислення водночас, що потенційно приводить до неймовірного збіль-

шення ефективності обчислень на відміну від класичних комп'ютерів. Є цілий ряд застосувань, де квантові комп'ютери принесуть особливі зміни:

- моделювання фізичних систем задля винайдення ліків і розроблення нових матеріалів;
- розв'язання комплексних проблем оптимізації в ланцюгах постачання, логістиці і фінансах;
- поєднання зі штучним розумом задля прискорення машинного навчання;
- факторизація цілих чисел, що дозволяє розшифровувати найбільш широко застосовані протоколи кібербезпеки, наприклад асиметричний алгоритм кодування, який застосовується для захищеного передавання даних RSA (Rivest–Shamir–Adleman).

Великі технологічні компанії, такі як IBM, Google і Microsoft, уже змагаються за «квантову перевагу» – момент, коли квантовий комп'ютер успішно розв'яже проблему, яку жоден класичний комп'ютер не зможе розв'язати за якийсь реальний проміжок часу. Це безпосередня загроза для суспільства загалом, а особливо для військових, зважаючи на важливість захищеного зв'язку і захищеної інформації для оборони та безпеки.

Квантові обчислення відкривають нові можливості у сфері кібербезпеки, хоча наразі вони ще перебувають у стадії активного дослідження. Основними напрямками застосування квантових обчислень у кібербезпеці є детекція та аналіз кіберзагроз, квантове шифрування, квантова криптографія, постквантова криптографія.

Детекція та аналіз кіберзагроз. Квантові комп'ютери можуть аналізувати величезні обсяги даних набагато швидше, ніж класичні комп'ютери, що дозволяє більш ефективно виявляти та аналізувати кіберзагрози. Застосування квантових обчислень для детекції та аналізу кіберзагроз – це новий й обіцяючий напрямок у галузі кібербезпеки. Використання квантових комп'ютерів може кардинально підвищити ефективність виявлення загроз та аналізу безпеки за допомогою таких можливостей:

- покращення швидкості обробки даних – квантові комп'ютери можуть виконувати деякі обчислювальні задачі значно швидше за класичні комп'ютери, завдяки їх здатності обробляти великі обсяги даних одночасно через квантову суперпозицію;
- квантовий пошук – алгоритми, такі як алгоритм Гровера, можуть забезпечити квадратичне прискорення в пошуку невпорядкованих БД, що може бути використано для швидшого знаходження шкідливих патернів або аномалій у даних;

- оптимізація – квантові алгоритми можуть допомогти в оптимізації складних систем безпеки, знаходження найкращих конфігурацій системи для максимальної ефективності захисту;
- розпізнавання образів – квантові обчислення можуть підвищити ефективність алгоритмів машинного навчання, які використовуються для розпізнавання шкідливих програм та ведення кіберзагроз;
- квантова стійкість – розроблення квантово-стійких алгоритмів і протоколів, здатних витримати потенційні атаки з використанням квантових комп'ютерів;
- аналіз квантових загроз – квантові комп'ютери самі можуть створювати нові типи загроз, тому необхідно розробити методи для виявлення та захисту від квантових атак;
- квантова криптоаналітика – квантові комп'ютери можуть зламати деякі із сучасних систем шифрування, включаючи RSA та ECC, що вимагає розроблення нових квантово-стійких шифрувальних методів.

Хоча квантові обчислення мають величезний потенціал у сфері кібербезпеки, їх застосування все ще перебуває на ранніх стадіях, і багато досліджень зосереджені на розробленні практичних технологій та систем, які можуть бути реалізовані в реальному світі.

Квантове шифрування. Це галузь квантової криптографії, яка використовує принципи квантової механіки для створення безпечних криптографічних систем. Розглянемо більш докладно основні види і типи квантового шифрування:

Квантове розподілення ключів. Це найбільш відомий і розвинений метод квантового шифрування. Він використовує квантові стани для безпечного розподілу криптографічних ключів між двома сторонами. Найважливішою особливістю QKD є те, що будь-яка спроба перехоплення або вимірювання цих квантових станів змінює їх, що може бути виявлено учасниками. Є два основних протоколи QKD: BB84 – розроблений Чарльзом Беннетом і Жилем Брассардом у 1984 році, що використовує одиничні фотони, поляризовані під чотирма різними кутами, і E91 – розроблений Артуром Екертом у 1991 році, що базується на заплутаних квантових станах.

Квантові алгоритми шифрування. Ці алгоритми використовують квантові обчислення для створення або розшифровки шифрованих повідомлень. Вони можуть бути надзвичайно потужними, здатними розкрити шифри, що є недосяжними для класичних комп'ютерів.

Квантові мережі. Це системи, які використовують квантове шифрування для захисту комунікації в мережах. Квантові мережі мо-

жуть інтегрувати QKD для забезпечення безпечного обміну ключами, що дозволяє створювати надійні, захищені від квантових атак канали зв'язку.

Квантове зберігання даних. Хоча це не прямий тип шифрування, розвиток квантових технологій зберігання даних може вплинути на способи шифрування та забезпечення безпеки інформації.

До переваг квантового шифрування можна віднести:

- теоретичну непробивність – за умови правильної імплементації, QKD може забезпечити майже абсолютний рівень безпеки;
- виявлення перехоплення – спроби несанкціонованого доступу можуть бути легко виявлені завдяки змінам у квантових станах;
- підготовку до майбутнього – квантове шифрування важливе для розвитку технологій, які зможуть протистояти квантовим комп'ютерам.

Викликами є:

- технічна складність – технології QKD є високо складними та дорогими в імплементації та експлуатації;
- обмеження дистанції – сучасні системи QKD мають обмеження по дальності дії, хоча ця проблема постійно вирішується завдяки новим дослідженням;
- швидкість передавання – швидкість передавання ключів в QKD може бути нижчою, ніж у традиційних методів.

Отже, квантове шифрування – це напрямок, що швидко розвивається й обіцяє змінити ландшафт кібербезпеки, але ще багато роботи потрібно зробити для його широкого впровадження.

Квантова криптографія. Включає розроблення нових криптографічних алгоритмів, які можуть протистояти атакам, використовуючи квантові комп'ютери. Такі алгоритми повинні бути стійкими до квантових атак, які можуть легко розшифровувати традиційні криптографічні схеми. Це напрям криптографії, який використовує особливості квантової механіки для забезпечення безпеки інформації. Основною відмінністю квантової криптографії від традиційної є використання квантових бітів, або кубітів, які можуть перебувати одночасно в кількох станах: як суперпозиція та квантова заплутаність, що дозволяє двом частинкам бути взаємопов'язаними незалежно від відстані між ними.

Основні аспекти квантової криптографії включають:

QKD. Це найбільш відомий протокол квантової криптографії. Він дозволяє двом сторонам створити спільний випадковий секретний ключ, який потім може бути використаний для шифрування і дешифрування повідомлень.

Квантова заплутаність. Це стан, де квантові системи, такі як фотони, стають кореляційно пов'язаними таким чином, що стан одного фотона миттєво впливає на стан іншого, незалежно від відстані між ними. Ця властивість використовується в QKD для виявлення спроб перехоплення, оскільки будь-яке вимірювання одного із заплутаних фотонів вплине на стан іншого.

Квантові геш-функції. Це спроба створення односторонніх криптографічних функцій, які можуть бути легко виконані в одному напрямку, але які надзвичайно важко обернути, використовуючи принципи квантової механіки.

Перевагами квантової криптографії є: висока стійкість (можливість виявлення будь-якої спроби перехоплення робить квантове шифрування дуже безпечним) та непробивність (деякі квантові криптографічні системи неможливо зламати, якщо вони виконані правильно).

А до викликів квантової криптографії можна віднести:

- технологічні обмеження – багато квантово-криптографічних систем усе ще перебувають на ранніх етапах розвитку й вимагають високоспеціалізованого обладнання;
- масштабування – розгортання цих систем на великі відстані; для багатьох користувачів є складним;
- інтеграцію – інтегрування квантової криптографії в існуючі інфраструктури безпеки вимагає значних зусиль.

Отже, квантова криптографія є обіцяючим напрямком у захисті інформації від майбутніх загроз, зокрема від квантових комп'ютерів, але її практичне застосування все ще вимагає значного технологічного прогресу.

Постквантова криптографія, або квантово-стійка криптографія – означає розроблення криптографічних алгоритмів, які мають бути стійкими до потенційних атак із використанням квантових комп'ютерів. Цей напрямок виник як відповідь на можливість, що квантові комп'ютери в майбутньому зможуть легко зламати алгоритми шифрування, які наразі вважаються безпечними, такі як RSA, DSA (Digital Signature Algorithm) та ECC (Elliptic Curve Cryptography), використовуючи алгоритм Шора, який дозволяє ефективно розкладати великі числа на прості множники.

Ключові аспекти використання квантових обчислень для розроблення та застосування постквантової криптографії:

Решіткова криптографія. Використовує математичні структури, відомі як решітки, для створення функцій, які важко інвертувати без спе-

ціального ключа. Прикладами є алгоритми, засновані на задачі найкоротшого вектора (Shortest Vector Problem, SVP) або найближчого вектора (Closest Vector Problem, CVP).

Хеш-базована криптографія. Використовує безпеку односторонніх хеш-функцій для створення підписів, які важко фальсифікувати без відповідного приватного ключа.

Код-базована криптографія. Базується на теорії корекції помилок і задачі декодування, вважається однією з найбільш перспективних для застосування в постквантовій ері.

Мультиваріативна криптографія. Використовує мультиваріативні поліноміальні рівняння як основу для створення криптографічних систем. Їх безпека полягає у складності розв'язання таких рівнянь.

Застосування у квантових обчисленнях. Використання квантових комп'ютерів для тестування. За допомогою квантових комп'ютерів можна тестувати стійкість розроблених алгоритмів до квантових атак, симулюючи можливі стратегії злому.

Дослідження нових криптографічних схем. Квантові обчислення можуть допомогти у відкритті нових математичних принципів та алгоритмів, які можуть бути використані для розроблення квантово-стійких криптографічних методів.

Викликами для постквантової криптографії є:

- масштабування – багато постквантових алгоритмів вимагають значно більших розмірів ключів порівняно з класичними алгоритмами, що може вплинути на швидкість та ефективність систем.
- доведення безпеки – не для всіх постквантових алгоритмів існують формальні доведення безпеки, тому вони потребують ретельного аналізу й тестування.

Отже, розвиток постквантової криптографії є важливим для підготовки до майбутньої ери квантових обчислень і для захисту інформації від нових квантових загроз. Квантові обчислення обіцяють принести революційні зміни в кібербезпеці, але важливо пам'ятати, що ця галузь усе ще знаходиться на ранніх етапах розвитку, і багато потенційних застосувань ще потребують дослідження та розвитку.

Основні загрози застосування квантових обчислень для кібербезпеки. Найбільшою загрозою від квантових обчислень є їхня здатність розшифровувати сучасні криптографічні алгоритми, які наразі вважаються безпечними. Алгоритми, такі як RSA і ECC, що використовуються для захисту більшості цифрових комунікацій, можуть бути легко зламані за допомогою достатньо потужних квантових комп'ютерів.

Квантові обчислення також становлять суттєві загрози для сучасної криптографії, зокрема для криптографічних систем, які базуються на математичних задачах, розв'язання яких є складним для класичних комп'ютерів, але може бути полегшеним для квантових машин. Ось найважливіші з них:

Злам шифрів із відкритим ключем. Багато сучасних криптосистем, які використовують асиметричне шифрування, такі як RSA, DSA та ECC, базуються на математичних задачах, які є важкими для розв'язання, – наприклад, факторизація великих чисел або визначення дискретних логарифмів. Квантові обчислення можуть розв'язувати ці задачі набагато ефективніше завдяки алгоритму Шора, що уможливлює злам цих шифрів.

Вплив на хеш-функції. Хеш-функції відіграють важливу роль у багатьох аспектах кібербезпеки, включаючи аутентифікацію та інтегрітет даних. Хоча квантові обчислення і не здаються такими загрозливими для хеш-функцій, як для шифрів із відкритим ключем, існує теоретична можливість, що вони можуть прискорити деякі види атак на хеш-функції.

Злам симетричного шифрування. Симетричне шифрування, яке використовує один і той самий ключ для шифрування та дешифрування, також може бути піддане підвищеному ризику через квантові обчислення. Алгоритм Гровера дозволяє квантовим комп'ютерам шукати в просторі ключів значно швидше, ніж це можливо класичними методами, хоча це не так катастрофічно, як алгоритм Шора для асиметричних шифрів.

Виклики для криптоаналізу. Квантові обчислення можуть використовуватися для вдосконалення криптоаналітичних методів, здатних виявляти слабкі місця в криптографічних алгоритмах, які раніше вважалися безпечними.

Отже, для протидії цим загрозам потрібен активний розвиток постквантової криптографії, який включає розроблення нових алгоритмів, що залишатимуться безпечними навіть у присутності потужних квантових комп'ютерів. Робота в цій сфері все ще триває, і немає єдиного стандарту, який був би широко прийнятий. Тому існує необхідність розроблення нових криптографічних методів, які будуть стійкими до атак із використанням квантових обчислень. Це вимагає значних зусиль у дослідженнях і розробленні, а також оновлення існуючих систем безпеки.

Якщо квантові комп'ютери стануть здатними розшифровувати зашифровані повідомлення, це може створити значні ризики для конфіденційності особистих, корпоративних та державних даних. Квантові обчислення впливають на проблему конфіденційності в кібербезпеці досить суттєво, і ось кілька ключових аспектів цього впливу:

Злам шифрування. Квантові комп'ютери здатні ефективно виконувати алгоритм Шора, який може зламати шифри, засновані на завданні факторизації великих чисел і визначенні дискретних логарифмів, такі як RSA і ECC. Це може призвести до компрометації конфіденційності даних, зашифрованих за допомогою цих методів.

Шифрування трафіку. Зараз багато інтернет-комунікацій захищені за допомогою протоколів шифрування, які в майбутньому можуть бути зламані квантовими комп'ютерами. Це ставить під загрозу конфіденційність історичного трафіку, який може бути перехоплений і збережений зараз для розшифровки в майбутньому.

Захист інформації. Квантові обчислення вимагають розроблення нових методів шифрування, які можуть захистити конфіденційність даних навіть перед обличчям квантових комп'ютерів. Це включає постквантову криптографію та квантове шифрування.

Загроза «збереження зашифрованих даних». Існує реальна загроза, що зловмисники можуть збирати і зберігати зашифровані дані сьогодні, чекаючи на майбутній розвиток квантових обчислень, які дозволять їм розшифрувати ці дані.

Правові та етичні виклики. Розвиток квантових технологій також порушує питання про використання та контроль над квантовими технологіями, а також про правові рамки для забезпечення конфіденційності та захисту даних.

Отже, для вирішення цих викликів важливо інвестувати в розвиток та імплементацію постквантових криптографічних систем та стандартів безпеки, які можуть забезпечити надійний захист інформації в епоху квантових технологій.

Квантові обчислення можуть суттєво вплинути на IT-інфраструктуру, оскільки вони змушують організації переосмислити та оновити свої системи безпеки, особливо в контексті криптографії. Ось основні чинники, через які виникає необхідність оновлення IT- інфраструктури:

Криптографічна стійкість. Багато сучасних криптографічних систем, які використовуються для захисту даних, не є стійкими до потенційних квантових атак. Оновлення цих систем до постквантових алгоритмів, які можуть протистояти квантовому декодуванню, є критично важливим.

Планування міграції. Організації мають розробити стратегічні плани для міграції своєї інфраструктури до нових, квантово-стійких технологій, які можуть включати оновлення апаратного забезпечення, програмного забезпечення та мережевих протоколів.

Зберігання даних. Потрібно переглянути методи зберігання даних, включаючи шифрування дискових просторів та інших носіїв інформації, щоб забезпечити їхню безпеку в умовах квантового майбутнього.

Захист комунікацій. Протоколи зв'язку, такі як TLS/SSL, можуть потребувати оновлення, щоб включати квантово-стійкі алгоритми шифрування, забезпечуючи безпечний обмін інформацією між серверами та клієнтами.

Стандартизація. Оновлення інфраструктури вимагатиме також впровадження нових стандартів і протоколів, які забезпечать уніфіковане та безпечне використання квантових та постквантових технологій.

Інвестиції в нові технології. IT-інфраструктура має бути оновлена не лише на рівні криптографії, але й в плані впровадження нових квантових технологій, які можуть використовуватися для покращення обчислювальних можливостей та ефективності аналізу даних.

Освіта та навчання. Необхідно буде оновити знання та навички IT-фахівців для роботи з новими квантово-стійкими технологіями та криптографією.

Ці виклики вимагають комплексного підходу та довгострокового планування, і організації, які почнуть підготовку до квантового майбутнього зараз, зможуть краще захистити свої активи і дані в майбутньому.

Отже, для впровадження квантово-стійких криптографічних систем потрібно буде оновити існуючу IT-інфраструктуру, що може виявитися дорогим та складним завданням для багатьох організацій. Але квантові обчислення можуть дати значні переваги, тому важливо вже зараз починати готуватися до викликів, які вони можуть принести у сфері кібербезпеки.

Нові досягнення в розробленні квантових технологій потенційно можуть принести нові захопливі можливості для військових. Зважаючи на значну зацікавленість і фінансування квантових технологій з боку як цивільної промисловості, так і урядів, очікується, що ці технології будуть розвиватись, і нові квантові застосування стануть доступними протягом найближчих п'яти – десяти років. Проте, для того щоб військові могли фактично користуватися перевагами цих нових квантових технологій, важливо, щоб вони активно долучалися до роботи в цій сфері та скеровували розроблення й упровадження військових застосувань квантових технологій. Військові можуть забезпечити значну додану вартість наявним зусиллям промисловості і науки, надавши інфраструктуру для тестування і випробувань (випробувальні центри), а також доступ до військових операторів, які будуть кінцевими користувачами. Якнайра-

ніші експерименти із цими технологіями не лише сприятимуть їхньому подальшому розвитку, але й допоможуть військовим ознайомитись із цими технологіями та їхніми можливостями, що полегшить подальше впровадження. Ба більше, активна участь у квантовій екосистемі покращує розуміння військовими потенційних ризиків, пов'язаних із квантовими технологіями, особливо в кіберсфері.

Підсумовуючи, зазначимо, що квантові технології швидко розвиваються і мають потенціал відкрити абсолютно нові можливості – трансформувати кібербезпеку й надати змогу розв'язувати проблеми, які раніше здавалися нерозв'язними. Водночас вони становлять серйозну загрозу кібербезпеці та обороні, тому як цивільні, так і військові організації повинні вже зараз уживати активних заходів для свого захисту. Для протидії цій загрозі також потрібно буде повністю вдосконалити нашу захищену цифрову інфраструктуру. Оцінюючи свої поточні протоколи кібербезпеки, досліджуючи перспективні технології та залучаючи поради експертів, вони зможуть краще підготуватися до захисту від майбутніх квантових загроз.

5.1.3. Біометричні технології

Біометрія належить до тих новітніх технологій, розвиток яких пришвидшився після відомих подій 11 вересня 2001 року в США [23]. Сучасні тенденції політичного світового розвитку вказують на те, що XXI ст. почалося з посилення конфронтації та боротьби за сфери впливу між різними державами. Ці конфлікти породжуються насамперед наявними відмінностями в політиці, економіці, культурі та релігії держав. Процес глобалізації разом із суттєвою зміною світової економіки став каталізатором стрімкого розвитку нелегальної міграції, тероризму та міжнародної організованої злочинності, зокрема кіберзлочинності. Тому актуальними стали питання адекватної реакції на негативні виклики сучасності та застосування новітніх технологій для забезпечення кібербезпеки.

Можна з упевненістю констатувати, що в реаліях сьогодення значно зростає кількість кібератак і кіберзлочинів, які посягають не лише на права і свободи окремих громадян чи заподіюють шкоду безпеці об'єктів критичної інфраструктури, а і становлять загрозу національній безпеці кожної держави в цілому. Тому в умовах сучасних глобалізаційних процесів та інформатизації суспільства потрібні нові перспективні технології кіберзахисту, зокрема біометричні [24].

У контексті цієї проблеми проводяться інтенсивні дослідження для розвитку основних прикладних сфер застосування біометрії – ідентифікації і верифікації особи. Особливо перспективним напрямом є розроблення та виробництво різних біометричних інтелектуальних систем безпеки [25, 26]. Біометричні системи ідентифікації охоплюють системи доступу за відбитками пальців і долонь, райдужною оболонкою ока, геометрією обличчя, малюнком вен на руці або пальці, дезоксирибонуклеїновою кислотою (ДНК), формою вуха, температурою шкіри, підписом та голосом. І це ще не повний перелік, який має стійку тенденцію до розширення. Далі розглянемо можливості застосування біометричних технологій у кіберзахисті більш докладно [27– 34].

Біометричні технології, засновані на відбитках пальців. Біометричні технології, особливо ті, що базуються на відбитках пальців, обіцяють значно змінити сферу кібербезпеки. За останніми дослідженнями та трендами, можна виділити декілька ключових напрямків розвитку та їх впливу на захист даних і систем:

персоналізований захист – відбитки пальців пропонують унікальний і неповторний спосіб ідентифікації особи, забезпечуючи високий рівень безпеки для особистих і корпоративних даних;

збільшення захищеності даних – біометрія, включаючи відбитки пальців, допомагає захистити дані від несанкціонованого доступу, знижуючи ризик витоку інформації;

інтеграція із цифровими сервісами – використання біометрії для доступу до електронних медичних записів та інших цифрових сервісів сприяє підвищенню кібербезпеки, роблячи процеси більш безпечними та зручними для користувачів;

розвиток технологій і зменшення ризиків – незважаючи на існуючі ризики обходу біометричних систем, наприклад, за допомогою високоякісних реплік, активно розвиваються нові покоління біометричних технологій, які мінімізують можливість таких атак;

протидія кібератакам – сучасні біометричні технології активно використовуються для захисту від кібератак, зокрема, за допомогою фінгерпринтингу, що є одним із найдавніших методів біометрії.

Очікується, що майбутні інновації в біометричних технологіях, зокрема, удосконалення ідентифікації за відбитками пальців, забезпечать ще більш надійний рівень кіберзахисту, інтегруючись із широким спектром пристроїв та сервісів.

Біометричні технології кібербезпеки, які базуються на відбитках пальців, розвиваються з метою подолання існуючих недоліків, таких як

вразливість до підробки та обмежена надійність у певних умовах. Ці технології планують вирішити існуючі проблеми за рахунок:

багаторівневої аутентифікації. Майбутнє біометрії обіцяє інтеграцію відбитків пальців з іншими біометричними методами, такими як розпізнавання обличчя та іридодіагностика, для створення більш складної та безпечної системи аутентифікації;

удосконалених датчиків. Покращення технологій датчиків дозволяє точніше зчитування відбитків пальців, знижуючи ймовірність помилок та підвищуючи стійкість до підробок. Це передбачає розроблення датчиків, які можуть розпізнавати глибші характеристики шкіри;

ШІ та машинного навчання. Застосування ШІ для аналізу відбитків пальців може допомогти виявити спроби обману, аналізуючи не лише зображення відбитка, але і його поведінку в динаміці. Це допомагає ідентифікувати підроблені або модифіковані відбитки;

криптографічного забезпечення. Захист даних відбитків пальців за допомогою сучасних криптографічних методів гарантує, що навіть у разі несанкціонованого доступу до біометричних даних їх буде складно використати для входу в систему;

постійного оновлення та адаптації. Біометричні системи безперервно оновлюються для адаптації до нових загроз та використання передових досліджень у галузі біометрії для підвищення їхньої ефективності та безпеки.

Таким чином, біометричні технології, засновані на відбитках пальців, зможуть значно покращити кібербезпеку, подолавши багато із своїх традиційних недоліків за допомогою інтеграції з іншими технологіями, удосконаленням датчиків, застосуванням ШІ та криптографії.

Біометричні технології, засновані на розпізнаванні обличчя. Обіцяють значне збільшення їхньої ролі в кібербезпеці. Розвиток цих технологій спрямований на забезпечення більш високого рівня безпеки для ідентифікації та аутентифікації користувачів у різних сферах, включаючи доступ до приватних даних, фінансові послуги, контроль доступу до приміщень та особистих пристроїв.

Основні аспекти майбутнього використання біометричних технологій розпізнавання обличчя:

покращення точності. Сучасні технології розпізнавання обличчя постійно вдосконалюються, щоб забезпечити високу точність ідентифікації, навіть у складних умовах, таких як низьке освітлення або коли обличчя частково прикрите;

*інтеграція з іншими системами***.** Технології розпізнавання обличчя інтегруються з іншими біометричними системами, такими як відбитки пальців та сканування сітківки ока, для створення багатофакторної аутентифікації, що забезпечує вищий рівень безпеки;

застосування в широкому спектрі сфер. Розпізнавання обличчя використовується не лише для захисту від несанкціонованого доступу до даних або систем, але й для покращення кібербезпеки в громадських місцях, забезпечуючи можливість виявлення та ідентифікації осіб, які можуть становити загрозу;

приватність та етичні питання. Розвиток технологій розпізнавання обличчя також порушує питання приватності та етики. Важливо забезпечити баланс між підвищенням безпеки та захистом особистих даних користувачів.

Загалом біометричні технології розпізнавання обличчя обіцяють значно вплинути на кібербезпеку, пропонуючи ефективніші та безпечніші методи ідентифікації та аутентифікації, одночасно зіштовхуючись із викликами щодо забезпечення приватності та етичного використання.

Біометричні технології кібербезпеки, засновані на розпізнаванні обличчя, активно розробляються, щоб подолати стандартні недоліки існуючих систем. Ці недоліки включають уразливість до шахрайства, зокрема використання фотографій або відео для обману системи, а також обмежену точність у складних умовах освітлення або при зміні зовнішності особи. Основні напрями розвитку цих технологій такі:

- покращення алгоритмів машинного навчання – майбутні системи використовуватимуть удосконалені алгоритми машинного навчання та ШІ для забезпечення більш точного розпізнавання облич, навіть у складних умовах, та для виявлення спроб обману;
- використання багаторівневої аутентифікації – інтеграція розпізнавання обличчя з іншими формами біометричної аутентифікації, такими як відбитки пальців та сканування райдужної оболонки, забезпечить додатковий рівень безпеки, допомагаючи подолати недоліки одного методу за допомогою переваг іншого;
- застосування глибокого навчання для виявлення живості – розроблення технологій виявлення живості, які можуть розрізняти реальну людину від фотографій або відео, допоможе запобігти шахрайству і значно підвищити безпеку систем;
- енкрипція біометричних даних – забезпечення безпеки зберігання та передання біометричних даних за допомогою сучасних методів шифрування допоможе запобігти їх витоку або несанкціонованому доступу.

Таким чином, використання вдосконалених технологій та підходів дозволить майбутнім біометричним системам кібербезпеки, заснованим на розпізнаванні обличчя, подолати їх стандартні недоліки та забезпечити високий рівень безпеки та надійності.

Біометричні технології, засновані на розпізнаванні голосу. Біометричні технології, що засновані на розпізнаванні голосу, обіцяють внести значні зміни у сферу кібербезпеки. Ці технології пропонують унікальний спосіб ідентифікації та аутентифікації особистості, виходячи з голосових характеристик, які важко підробити чи відтворити, зокрема:

- вдосконалення точності та надійності – майбутні розробки в галузі розпізнавання голосу зосереджуватимуться на покращенні точності розпізнавання, зменшенні помилок та підвищенні стійкості до спроб обману, використовуючи складні алгоритми машинного навчання та ШІ;
- багаторівнева аутентифікація – інтеграція голосової біометрії з іншими біометричними методами, такими як відбитки пальців або розпізнавання обличчя, дозволить створювати більш надійні системи багаторівневої аутентифікації, підвищуючи загальний рівень безпеки;
- застосування в широкому спектрі сфер – від фінансових послуг до контролю доступу та особистих асистентів, розпізнавання голосу стане важливою частиною багатьох систем кібербезпеки, забезпечуючи зручний та безпечний спосіб взаємодії із цифровими сервісами;
- виклики та питання приватності – подальший розвиток та впровадження голосової біометрії повинні враховувати питання приватності та захисту даних, а також розробляти заходи для захисту від несанкціонованого доступу або використання біометричних даних.

Таким чином, майбутнє голосової біометрії в кібербезпеці виглядає обнадійливим, пропонуючи більш безпечні та зручні способи аутентифікації, при цьому висуваючи нові виклики для захисту приватності та особистих даних користувачів.

Біометричні технології кібербезпеки, зокрема ті, що базуються на розпізнаванні голосу, розробляються з метою подолання стандартних недоліків, таких як висока частка помилкових спрацьовувань та потенційна вразливість до шахрайства. Яким чином вони планують це зробити:

- покращення алгоритмів машинного навчання – використання розширених алгоритмів машинного навчання та ШІ дозволить точніше аналізувати голосові відтінки, знижуючи ймовірність помилкових спрацьовувань та підвищуючи точність ідентифікації;

• застосування багатофакторної аутентифікації – інтеграція голосової біометрії з іншими формами аутентифікації, такими як відбитки пальців або розпізнавання обличчя, забезпечить додатковий рівень безпеки, зменшуючи ризик шахрайства;

• використання глибинного навчання для виявлення живості – розроблення технологій виявлення живості, заснованих на глибинному навчанні, допоможе відрізняти живий голос від записів або синтезованих голосів, значно підвищуючи безпеку системи;

• покращення захисту даних – використання сучасних методів шифрування та безпечного зберігання біометричних даних допоможе захистити інформацію про голос користувача від несанкціонованого доступу або викрадення.

Таким чином, розвиток технологій розпізнавання голосу в кібербезпеці спрямований на забезпечення вищого рівня захисту та надійності, водночас долаючи існуючі виклики та недоліки.

Біометричні технології, засновані на розпізнаванні сітківки ока. Технологія розпізнавання сітківки є однією з найбільш точних форм біометричної ідентифікації, оскільки сітківка ока кожної людини є унікальною та не змінюється із часом. Вона обіцяє значне посилення кібербезпеки.

Розпізнавання сітківки ока вирізняється високою точністю і низькою ймовірністю помилок, що робить її ідеальною для застосування в критичних системах безпеки. Такі технології широко використовуються у фінансовій сфері та охороні здоров'я для забезпечення безпеки доступу до конфіденційної інформації та медичних записів, знижуючи ризик шахрайства та несанкціонованого доступу. Розвиток технологій сканування та алгоритмів обробки даних сприятиме ще більшому покращенню точності та швидкості розпізнавання, а також забезпеченню зручності використання для кінцевих користувачів.

Незважаючи на численні переваги, розвиток та впровадження технологій розпізнавання сітківки ока також ставлять питання про захист персональних даних і приватності. Важливо розробити відповідні правила та норми для захисту біометричних даних.

Таким чином, майбутнє біометричних технологій, заснованих на розпізнаванні сітківки ока, виглядає обнадійливим із точки зору посилення кібербезпеки. Однак важливо забезпечити належний захист приватності та персональних даних при їхньому впровадженні та використанні.

Біометричні технології кібербезпеки, засновані на розпізнаванні сітківки ока, мають потенціал подолати низку стандартних недоліків,

пов'язаних із точністю, безпекою та приватністю. Ці технології надають унікальні можливості для ідентифікації особи, використовуючи унікальні характеристики сітківки ока, яка вважається однією з найбільш точних форм біометричної ідентифікації.

Майбутні технології, засновані на розпізнаванні сітківки ока, будуть використовувати розширені алгоритми та методи машинного навчання для покращення точності розпізнавання та зниження відсотка помилкових спрацьовувань. Удосконалені системи розпізнавання сітківки ока передбачатимуть функції виявлення спроб підробки, зокрема використання фотографій або відеозаписів, що значно підвищить рівень безпеки та забезпечить кращий захист від підробки та шахрайства.

Майбутні системи будуть оснащені передовими технологіями шифрування та захисту даних, щоб забезпечити конфіденційність біометричної інформації та захист від несанкціонованого доступу. Для забезпечення багаторівневої безпеки та підвищення надійності, розпізнавання сітківки ока може бути інтегроване з іншими біометричними технологіями, такими як відбитки пальців або розпізнавання обличчя, створюючи комплексну систему ідентифікації.

Таким чином, майбутнє біометричних технологій, заснованих на розпізнаванні сітківки ока, обіцяє значне поліпшення в кібербезпеці, зокрема в точності ідентифікації, захисті від шахрайства, приватності даних та інтеграції з іншими системами безпеки.

Біометричні технології, засновані на розпізнаванні ДНК. Біометричні технології, що засновані на розпізнаванні ДНК, відкривають нові перспективи для кібербезпеки, пропонуючи надзвичайно точні та безпечні способи ідентифікації осіб. Розпізнавання ДНК має потенціал стати одним із найбільш надійних методів біометричної ідентифікації завдяки унікальності ДНК кожної людини.

ДНК-біометрія вирізняється своєю високою точністю та майже неможливістю підробки. Це забезпечує винятковий рівень безпеки для ідентифікації особи, що є критично важливим для захисту від шахрайства та несанкціонованого доступу. Незважаючи на високу точність, використання ДНК для біометричної ідентифікації має свої виклики, зокрема, схильність ДНК до деградації та контамінації. Майбутній технологічний розвиток спрямований на вирішення цих проблем, щоб забезпечити надійне та довгострокове зберігання біометричних даних.

Одним з основних питань, що виникають при використанні ДНК для біометричної ідентифікації, є захист приватності та персональних даних. Розроблення безпечних протоколів та систем зберігання даних,

що виключають несанкціонований доступ, є ключовим елементом майбутнього використання ДНК у кібербезпеці.

ДНК-біометрія може знайти застосування в багатьох сферах – від кібербезпеки фінансових установ до контролю доступу в особливо захищені зони. Це дозволить створити більш безпечне та надійне середовище в різних галузях.

Загалом майбутнє ДНК-біометрії обіцяє стати революційним кроком у сфері кібербезпеки, пропонуючи безпрецедентний рівень точності та безпеки ідентифікації, при цьому висуваючи нові виклики для захисту приватності та персональних даних. Біометричні технології кібербезпеки, засновані на розпізнаванні ДНК, обіцяють подолати низку стандартних недоліків, притаманних більш традиційним біометричним системам, таких як відбитки пальців, розпізнавання обличчя або сітківці ока. Використання ДНК для біометричної ідентифікації може значно підвищити безпеку завдяки унікальності та складності ДНК кожної людини.

ДНК має величезний потенціал для ідентифікації осіб із неперевершеною точністю, оскільки ДНК кожної людини є унікальною. Це мінімізує ризик помилкових збігів або шахрайства. Біометричні системи, що використовують лише один тип біометричних даних, можуть мати обмеження, такі як чутливість до зовнішніх умов або можливість обходу. ДНК-розпізнавання може працювати ефективно в комбінації з іншими методами для створення багатофакторної аутентифікації, підвищуючи загальний рівень безпеки.

З огляду на важливість та чутливість ДНК як біометричного ідентифікатора, майбутні технології розроблятимуться з передовими механізмами шифрування та захисту даних, щоб запобігти несанкціонованому доступу або зловмисному використанню. З розвитком ДНК-розпізнавання виникнуть питання етики та приватності, які потребуватимуть вирішення через розроблення відповідних правових рамок та політик для захисту особистих біометричних даних. Ураховуючи ці аспекти, майбутні біометричні технології на основі ДНК мають потенціал значно підвищити рівень кібербезпеки, одночасно вирішуючи виклики, пов'язані з точністю, безпекою даних та приватністю.

Отже, розширення сфери застосування біометричних технологій насамперед пов'язане з постійно зростаючою потребою державних органів і бізнесу в забезпеченні безпеки, із вразливістю персональних комп'ютерів, існуючих інформаційних мереж та безупинним зростанням кіберзлочинності. Біометричні технології в кібербезпеці обіцяють стати ще більш інноваційними та інтегрованими в наше повсякденне

життя. Вони передбачатимуть розширені методи аутентифікації, засновані на унікальних фізичних або поведінкових характеристиках людини, таких як відбитки пальців, розпізнавання обличчя, голосу, сітківки ока та навіть ДНК. Очікується, що з подальшим розвитком ШІ та машинного навчання ці технології стануть ще точнішими та безпечнішими, мінімізуючи ризики помилкових позитивних або негативних результатів. Одним із напрямків, який може відіграти ключову роль, є поведінкова біометрія, що аналізує унікальні способи взаємодії людини з пристроями, наприклад, патерни набору тексту, рухи мишкою чи спосіб ходьби. Це дозволяє створити динамічний профіль користувача, що змінюється разом із ним, забезпечуючи високий рівень безпеки без необхідності постійної фізичної взаємодії. Також велику увагу потрібно приділяти розробленню безконтактних біометричних технологій, які гарантують безпеку та зручність використання без необхідності фізичного дотику. Зі зростанням кіберзагроз і зловмисних атак біометричні технології стануть невід'ємною частиною засобів кібербезпеки, які дозволять підвищити рівень захисту особистих і корпоративних даних.

5.2. Операційна система кібербезпеки

Одним із найсучасніших засобів захисту корпоративного рівня є Security Operation Center (SOC). Сьогодні в Україні вже існує кілька SOC, зокрема і комерційних, але питаннями їхньої побудови також цікавляться інші державні організації та підприємства практично всіх галузей вітчизняної економіки. Цей інтерес викликаний насамперед кібератаками, що постійно вдосконалюються, і потребою в сучасних засобах протидії. Дійсно, SOC є ефективним засобом забезпечення інформаційної та кібербезпеки будь-якої організації, що дозволяє здійснювати моніторинг, детектування та оперативну реакцію на інциденти безпеки.

Слід зазначити, що побудова SOC потребує значних матеріальних витрат, які не всі організації можуть собі дозволити, а також досить тривалого часу. Тому створення аналогічного засобу, а саме – Операційної Системи Кібербезпеки (ОСК), допомогло б вирішити завдання забезпечення кібербезпеки організацій у більш короткі терміни та з меншими фінансовими витратами [35].

Проведений аналіз наявності та експлуатації промислових систем інформаційної та кібербезпеки вітчизняними організаціями корпоративного рівня показав, що в середньому використовується понад 20 класів таких систем (рис. 5.3).

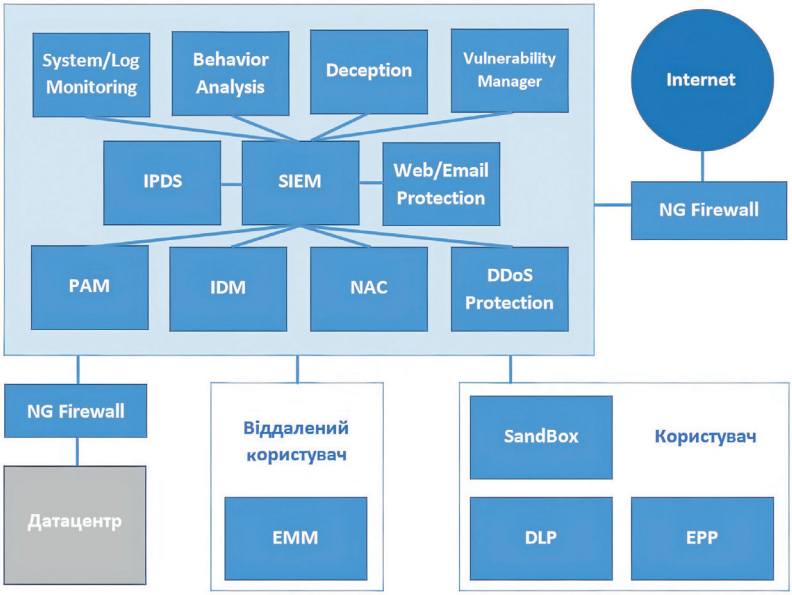

Рис. 5.3. Системи корпоративної інформаційної та кібербезпеки організації

Це не означає, що всі вони обов'язково повинні бути впроваджені для досягнення «повної безпеки», але це демонструє, наскільки широкий «фронт» кібервійни та наскільки можна формувати ландшафт кібербезпеки, тому що для неї вже є необхідний базис. Звісно, за такої умови не всім організаціям потрібен WAF та antiDDoS, не всі ще доросли до мікросегментації на рівні гіпервізора, не всі процеси вимагають / дозволяють «ввести» Identity Management.

Спочатку спробуємо відповісти на запитання: «Чим відрізняються два поняття – інформаційна безпека та кібербезпека?». Відповідь можна сформулювати таким чином: інформаційна безпека – це захист даних від різноманітних навмисних, випадкових, природних / стихійних та інших несанкціонованих маніпуляцій даними (доступ, знищення, спотворення, перешкоджання доступу тощо), а кібербезпека – це захист комп'ютерів, мереж, програмних додатків, критично важливих систем та даних від потенційних кіберзагроз та кібератак.

Таким чином, якщо інформаційна безпека включає резервне копіювання і відновлення архівування, план безперервності бізнесу (BCP) і відновлення після збою (DRP), тобто займається збереженням корпора-

тивної інформації й можливістю її обробляти, то кібербезпека стосується таких понять, як: віруси, програмні вразливі місця, витік даних, атаки з відмовою в обслуговуванні (DDoS), вимагання викупу, фішинг та інші, які спрямовані на компрометацію даних, розрив сервісу та крадіжку ураженої інформації.

Попри те, що ці поняття досить тісно пов'язані, вони таки мають певні відмінності та свою специфіку. Далі розглядатиметься саме кібербезпека та синергія трьох її компонентів: технічних засобів, процесів та фахівців (рис. 5.4).

Рис. 5.4. Компоненти кібербезпеки

Сучасні атаки найчастіше багатовекторні та поетапні, тобто починаються з вибору вектора атаки, який дасть змогу «пройти» периметр й отримати доступ до тієї чи іншої інформаційної системи. Проходження периметра зараз є лише першим етапом атаки, а не її апофеозом, адже давно минув той час, коли надійний периметр уважався гарантією безпеки IT-інфраструктури, та й саме поняття периметра інформаційної безпеки втратило свою цілісність та монолітність унаслідок тенденцій розвитку сучасних технологій.

З огляду на це неурядова організація MITRE Corporation розробила модель ATT&CK, що описує поетапність, процес та техніки атак і компрометації корпоративних мереж [36]. Згідно із цією моделлю, процес вторгнення та виконання шкідливих дій складається з декількох етапів, які зображено на рис. 5.5.

Якщо не брати до уваги стадію підготовки, то атака складається з кількох етапів, які передбачають: доставлення шкідливого вмісту, зараження, узяття атакованої системи під управління, виконання руйнівних дій, закріплення та розширення.

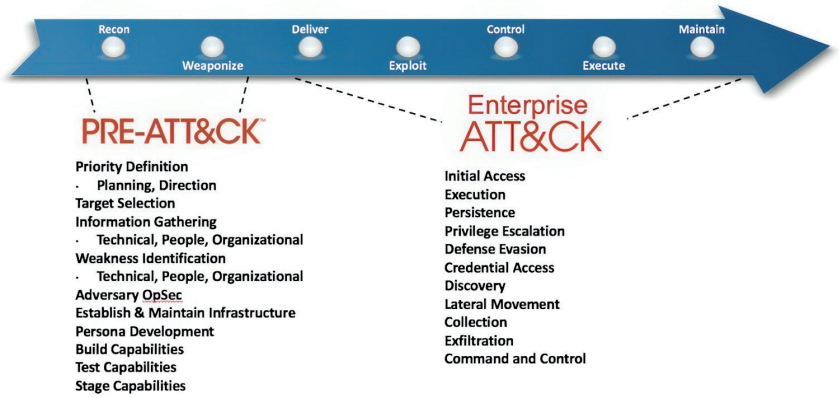

Рис. 5.5. Модель ATT&CK

За інформацією від компанії-виробника Cisco Systems – світового лідера в галузі мережевих технологій, тривалість злому до проникнення становить хвилини, до виконання шкідливих дій можуть проходити хвилини, години, а часом – дні, а ось до виявлення проникнення та результатів атаки минають тижні, місяці, а іноді – роки. З огляду на це після того, як нападник, пройшовши периметр, уже проник усередину IT-інфраструктури, захист має одиниці-десятки хвилин на те, щоб запобігти шкідливим діям, а при концепції безпеки, яка все ще існує, орієнтованій на захист периметра, до виявлення проходять місяці, а іноді й роки.

Для того, щоб встигнути відреагувати на дії зловмисника, усередині периметра необхідно:

- уповільнити зловмисника, створивши для нього велику кількість помилкових цілей-приманок в IT-інфраструктурі;
- відстежувати активні чи шкідливі дії щодо створених приманок;
- зібрати максимально можливу інформацію про мережевий трафік усередині периметра для пошуку нетипової поведінки;
- зібрати журнали та події IT-підсистем, зокрема інфраструктурних та особливо підсистем безпеки;
- провести нормування, аналіз та кореляцію подій та логів;
- виявити нетипову або небезпечну поведінку та провести розслідування й усунення інциденту.

Виходячи з вищеописаного, для своєчасної реакції на вторгнення, коли периметр уже подоланий зловмисниками, крім наявності стандартних засобів безпеки (антивірус/EPP/EDR, MME наступного покоління, систем безпеки електронної пошти та доступу до WEB, систем керу-

вання доступом до мережі тощо), для ефективного відображення сучасних атак необхідні збирання та централізований аналіз подій усередині IT-інфраструктури. Зважаючи на те, що в мережі середніх розмірів обсяг записів про події за добу може досягати десятків гігабайт, перегляд цих подій та їхній аналіз є дуже трудомісткими, що посилюється різною структурою повідомлень, різними рівнями критичності тощо. Саме для цих цілей використовуються системи Security Information and Event Management (SIEM), завданням яких і є збирання логів із систем, їхня нормалізація, знаходження підозрілих дій і залежностей для повідомлення про них фахівцю з безпеки як про подію (вдалий, невдалий або тривалий злом).

Але будь-який засіб збирання та аналізу інформації не є ефективним, якщо недостатньо даних для аналізу. На вхід аналітичного інструментарію має надходити інформація про різні події та процеси в IT-інфраструктурі. Особливо цінною є інформація про мережеву активність, про знайдене ШПЗ, про спрацювання правил безпеки модулів запобігання вторгненням, а також про спрацювання пасток-приманок.

Для вирішення цього завдання необхідно визначити мінімально необхідний набір систем та пристроїв, який дозволить забезпечити базовий рівень безпеки IT-інфраструктури. Безумовно, базовий – «виконавчий» набір систем кібербезпеки повинен бути присутнім в IT-інфраструктурі організації. Термін «виконавчий» акцентує на тому, що ці системи виконують кожна свою роль у розв'язанні завдання кіберзахисту, і при цьому вони не забезпечують додаткового інтелекту, що інтегрує або аналізує, а просто захищають конкретні типи систем від конкретних типів атак. До списку таких обов'язкових систем належать:

- Next Generation Firewall (NGF);
- Endpoint Protection (EPP) / Antivirus або Endpoint Detection&Response (EDR);
- System/Log Monitoring;
- Netflow Analyzer;
- Threat Intelligence;
- Deception.

Це базовий набір, і він може бути розширений залежно від специфіки IT-інфраструктури організації та функціональних завдань. Ці системи, крім своїх прямих функцій, генерують і передають в аналітичну / корелюючу систему інформацію про специфічні події безпеки саме для цієї системи кібербезпеки для об'єднання в єдину БД і виконання аналізу.

Як централізоване аналітичне ядро системи корпоративної кібербезпеки виступає система збирання та аналізу логів та подій – SIEM, яка збирає події з доступного набору систем, нормалізує їх та проводить аналіз, кореляцію сукупностей подій, а також надання команді кібербезпеки результатів аналізу у вигляді рекомендацій, висновків та подій.

Для розуміння процесів, що відбуваються в мережі організації, дані про трафік (включаючи дані про 4-й рівень моделі OSI) треба знімати не лише з прикордонних маршрутизаторів та NGF, але і з мережевих пристроїв у вузлових точках, а для розуміння процесів у всіх сегментах – бажано з усіх мережевих пристроїв. Прикладом можуть бути дані, одержані Netflow, причому необхідна інформація про всі пакети, а не Sampled варіант. Збирати та аналізувати всю первинну інформацію NetFlow можна безпосередньо в SIEM або попередньо виконувати передобробку Netflow на collector / analyzer, або використовувати для аналізу систему типу Threat Intelligence з підключенням Behavior Analysis та хмарних аналітичних систем. Конкретне рішення залежить від наявного IT-ландшафту, завдань, обсягу мережі та типу / інтенсивності трафіку й обирається на етапі проєктування.

Для обробки та кореляції подій та процесів в IT-системах (сервера, СЗД, ОС, додатки тощо) необхідне оброблення журналів подій із додатків, гіпервізорів, БД, апаратних платформ тощо. Для цього такі події можуть спрямовуватися в SIEM безпосередньо та можуть здійснюватися збирання та попереднє оброблення в syslog або SNMP (Simple Network Management Protocol) серверах. Для виявлення ознак успішного вторгнення в мережу та ідентифікації шкідливого коду використовуються системи класу «пастки», які провокують зловмисника на активні дії проти створеної обманної псевдосистеми, яка має всі ознаки «жертви», але при цьому невідома легітимним користувачам і потрібна лише для того, щоб відстежувати спроби атак на неї та повідомляти системі кібербезпеки деталі про зловмисників та про тип / спосіб атаки. З погляду запобігання злому IT-систем, дуже ефективним способом є аналіз IT-систем на відомі вразливості за допомогою систем класу «сканер уразливості». Таке періодичне сканування дозволяє визначити, які із систем потенційно вразливі для тих чи інших класів атак, та завчасно вжити заходів для захисту.

Очевидно, що чим більше IT-систем будуть передавати інформацію про події та активності на систему кібербезпеки, тим більш комплексний аналіз буде виконано і більше кореляційних правил буде застосовано, а це своєю чергою дозволить команді безпеки забезпечити повну «видимість» процесів в IT-інфраструктурі організації та дій зловмисників.

Для визначення потенційного інциденту кібербезпеки, як зазначалося вище, необхідно провести аналіз та кореляцію по великій кількості подій та даних, які дозволяють отримати повну картину процесів та подій. З боку аналізу подій у кібербезпеці саме методи обробки BigData на предмет виявлення аномалій у поведінці користувачів, подій або трафіку відповідають концепції ШІ / машинного навчання (artificial intelligence / Machine Learning, AI/ML) [37].

Ця технологія демонструє дуже високу ефективність у задач визначення аномалії в будь-яких послідовностях або масивах даних. ML використовується для визначення підозрілої аномалії будь-якої природи та для аналізу наявності або вірогідності потенційної атаки на основі визначених подій, фактів, трендів та аномалії.

Для реалізації завдання визначення аномалій у трафіку корпоративної мережі, аномалій у трафіку Інтернет (визначення та боротьба с DDoS-атаками), аномалій у поведінці користувачів використовується метод машинного навчання без учителя. Система збирає дані за певний час та будує профіль поведінки кожного користувача або трафіку, що розглядається як норма, відносно якої визначається аномалія.

Ця інформація оброблюється в режимі квазіреального часу за методом Isolated Forest (IForest) чи Extended Isolated Forest (рис. 5.6).

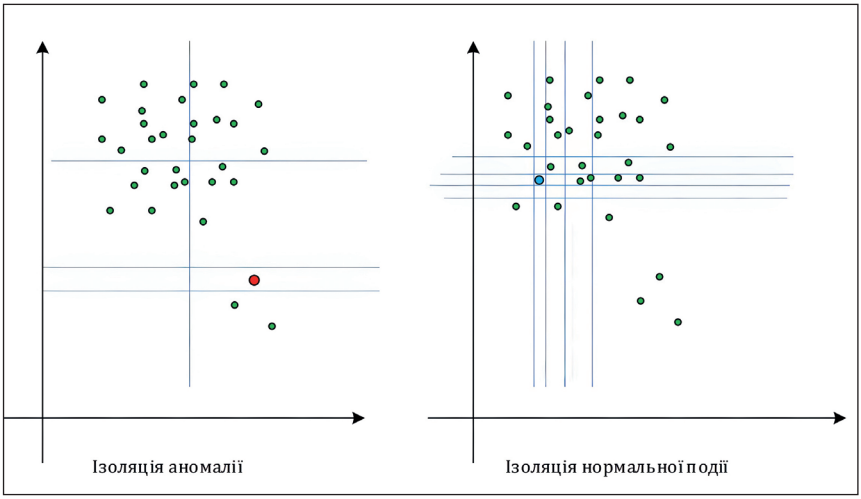

Рис. 5.6. Обробка інформації в режимі квазіреального часу за методом Isolated Forest (IForest)

Залежно від типу оцінюваної аномалії задають гіперпараметри – кількість «дерев» у «лісі», глибина «дерева», передбачувана доля аномалії в наборі даних, мінімальна вибірка до поділу та ін. Ці гіперпараметри задані в системі й можуть підбиратися шляхом аналізу як результат процесу перебору, але адміністратор також може змінювати їх залежно від існуючого ландшафту.

Використання ML для аналізу подій та даних або виявлених аномалій з метою визначення ймовірної атаки (інциденту кібербезпеки) базується на відомій матриці MITRE ATT&CK, яка класифікує відомі атаки та описує їх з точки зору векторів атаки та засобу використання їх для здійснення атак (розділ Detection). Після обробки матриці MITRE ATT&CK система ML отримує нормалізовану матрицю значної кількості атак, яка використовується як ландшафт для роботи моделі. Також система отримує з аналітичних систем та систем кібербезпеки події кібербезпеки, які визначені системою з ймовірністю, заданою відповідним гіперпараметром алгоритму, та використовує їх як ознаку / характеристику для моделі. Завдання алгоритму – використати ознаки (поточні факти та події) з урахуванням їхньої ймовірності для класифікації ймовірної атаки (за матрицею MITRE ATT&CK) та визначити її ймовірність. Після визначення ймовірності певного інциденту кібербезпеки (*Pi*) визначається пріоритет (*Pr*), тобто можлива небезпека цього потенційного інциденту з урахуванням наперед заданого індексу небезпеки інциденту (*Pv*):

$$Pr = 1 - (1 - m \cdot Pi) \cdot (1 - n \cdot Pv),$$

де:

Pr – пріоритет інциденту (діапазон: 0 – 1, більше – важливіший),

Pi – ймовірність наявності певного інциденту (діапазон: 0 – 1),

Pv – індекс небезпеки певного інциденту (діапазон: 0 – 1, більше – небезпечний),

m, n – відповідні вагові коефіцієнти, гіперпараметри.

Далі отримані пріоритети ранжують за методом скорингу, після чого k найбільш пріоритетних інцидентів передаються на розгляд команди ОСК. У наперед заданих випадках (конкретних типах або залежно від рівня *Pr)*, коли існує висока вірогідність критичної небезпеки, запускають автоматизовану послідовність реакції на атаку в системі оркестрації та автоматизації реакції на інциденти (SOAR).

Таким чином, використання систем машинного навчання для визначення та пріоритизації інцидентів кібербезпеки дозволяє різко знизити кількість подій безпеки, які треба обробляти команді ОСК. При цьому наявність інциденту визначається ШІ серед кількох тисяч потенційних

інцидентів з урахуванням усієї доступної інформації про події, тренди та факти, а не залежить лише від написаного кореляційного правила або опиту аналітику ОСК. Крім того, інциденти подаються аналітику ОСК уже з виставленим пріоритетом з урахуванням вірогідності самого інциденту та його небезпеки. Зазвичай використання системи штучного інциденту для обробки такого значного масиву даних у кілька етапів із виявлення аномалії та визначення вірогідності настання одного або кількох інцидентів серед багато тисяч потенційних потребує значної обчислювальної потужності. Тому апаратне забезпечення ОСК потребує аналізу та розроблення зазвичай на базі серверів із кількома графічними адаптерами (GPU), на яких і обробляються алгоритми AI/ML.

Ще одним компонентом кібербезпеки є процеси та процедури, які чітко описують для кожного члена команди кібербезпеки дії та подальші кроки в разі тієї чи іншої ситуації, таймінг та рівні ескалації, процедури взаємодії та залучення фахівців.

Процеси та процедури в службі корпоративної кібербезпеки, як і в будь-якій службі швидкого реагування, спрямовані насамперед на швидке та ефективне усунення інциденту та його наслідків, а по-друге, що не менш важливо, на підготовку команди та IT-інфраструктури до роботи в постійно мінливих умовах, і тому діляться, щонайменше, на три типи документів: Emergency, Routine, Escalation для кожної укрупненої ролі фахівців у команді.

Саме фахівці є найціннішим активом будь-якої служби кібербезпеки. Недарма зараз у світі спостерігається стійкий дефіцит цих фахівців, який, за деякими оцінками, у 2025 році досягне 4 млн незаповнених вакансій [10]. Як правило, склад команди кібербезпеки визначається на основі штатного розпису й формується залежно від обсягу IT-інфраструктури організації, необхідного графіка роботи та вимог до компетенції кожного члена команди.

З урахуванням вищевикладеного, для організації ефективного захисту від кіберзагроз та кібератак пропонується розроблена архітектура ОСК, яка дозволяє здійснювати збирання, нормалізацію та кореляційний аналіз подій в IT-інфраструктурі організацій, а також автоматизувати процес розслідування кіберінцидентів та реакції на атаки [38].

ОСК має такі складові (рис. 5.7):

- програмно-апаратний комплекс (ПАК) аналітичної платформи Splunk Enterprise з модулем Enterprise Security;
- ПАК платформи автоматизації та оркестрації розслідувань і реакції на інциденти Splunk SOAR;

- системи кібербезпеки, що входять до базового – «виконавчого» набору та доналаштовуються при побудові ОСК.

ОСК дозволяє реалізовувати основні процеси, що забезпечують кіберзахист:

- збирання логів, Netflow, статистики;
- аналіз зібраної інформації та її кореляцію;
- визначення поточних шкідливих дій;
- виявлення можливих атак та підозрілих дій;
- формування в автоматичному або автоматизованому режимі реакції на атаки; усунення наслідків атак;
- усунення виявлених «проломів» у безпеці.

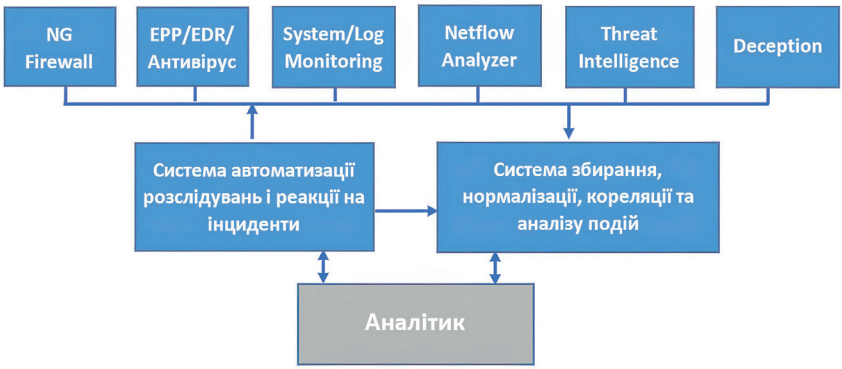

Рис. 5.7. Складові ОСК

Упровадження ОСК проводиться в такій послідовності:

- обстеження наявної IT-інфраструктури організації;
- прояснення та узгодження найбільш небезпечних векторів атак та найбільш уразливих / цінних IT-ресурсів;
- модернізація існуючих систем інформаційної та кібербезпеки організації до базового рівня (якщо це потрібно);
- встановлення та інсталяція ПАК збирання, нормалізації, кореляції та аналізу подій;
- встановлення та інсталяція ПАК автоматизації та оркестрації розслідувань і реакції на інциденти;
- розроблення та впровадження політики, процесів інструкцій, їх адаптація для конкретних умов на всіх етапах моделі ATT&CK (Predict, Prevent, Detect, Response);
- навчання штату IT-безпеки.

Основна перевага ОСК – це можливість отримання інформації про події з різних джерел та їхній кореляційний аналіз (200+ кореляційних правил), адже сучасні кібератаки та кіберзагрози можна виявити лише за сукупністю подій, що відбуваються в IT-інфраструктурі організації, і практично неможливо за окремими подіями в окремих системах інформаційного та кіберзахисту.

Необхідно також пам'ятати, що безпека – це не стан, а постійний процес адаптації триєдиної системи (технічні засоби, процеси, фахівці), який здійснюється ітераційно, з метою запобігти або мінімізувати шкоду від впливу кіберінцидентів на функціонування IT-інфраструктури організації (рис. 5.8).

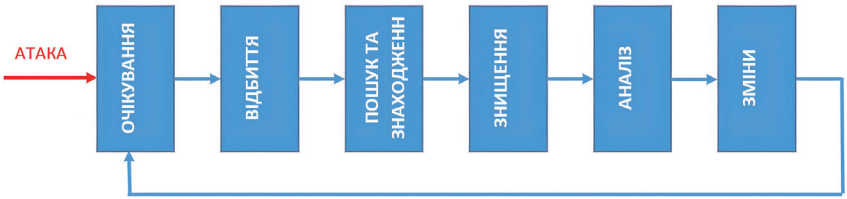

Рис. 5.8. Ітераційний процес адаптації ОСК

Отже, запропонована ОСК дозволяє забезпечити ефективний захист IT-інфраструктури організації від кібератак та кіберзагроз унаслідок отримання інформації про події та інциденти безпеки з різних джерел та проведення їхнього кореляційного аналізу. Водночас значно підвищується ефективність аналізу подій безпеки завдяки обробці аналітиком тільки інцидентів безпеки, а не всього потоку журналів подій і Netflow за допомогою ШІ.

Також доступна повна «видимість» процесів та подій в IT-інфраструктурі організації; з'являється можливість аналізувати та локалізувати інциденти безпеки як усередині, так і на периметрі мережі; істотно підвищується швидкість реакції та обробки кіберінцидентів завдяки використанню системи автоматизації розслідування і реакції на інциденти та роботі команди згідно з розробленими й адаптованими інструкціями та протоколами, із чіткими ролями. Крім того, при функціоналі ОСК аналогічному функціоналу SOC вартість її побудови на 15–20 % дешевше, а термін впровадження на 3 місяці менше.

5.3. Корпоративна система інформаційної та кібербезпеки

На сьогодні, коли кіберзагрози стають усе більш складними та поширеними, організації й установи повинні виявляти підвищену активність у забезпеченні безпеки. Успішна кібератака може призвести до серйозних наслідків, і не лише до миттєвих збитків, а й до довгострокової шкоди та юридичних наслідків. З удосконаленням кіберзлочинців, які використовують як технологічні, так і людські вразливості, організаціям і підприємствам важливо випереджати потенційні атаки, а цю можливість має давати корпоративна система інформаційної та кібербезпеки (КСІК) [39]. При цьому як результат забезпечується захист корпоративної інформаційної системи (КІС) організації від великої кількості різноманітних загроз, безперервність процесів електронної обробки інформації, мінімізуються порушення їхнього функцінування та життєдіяльності [40].

5.3.1. Компоненти КСІК

Раніше вважалося, що наявність ММЕ вирішує майже 90 % проблем, пов'язаних із можливими атаками на КІС, і для базового рівня захисту достатньо МСЕ наступного покоління на периметрі та антивірусів, установлених на робочих станціях та серверах [41]. Однак поряд зі зростанням цінності вмісту КІС, збільшення залежності від даних та їхньої доступності зростає і попит на розвиток технологій, методів та засобів кібератак. Сьогодні арсенал засобів та способів отримання чи знищення інформації в КІС величезний та оновлюється щодня. Крім класичних засобів, що дозволяють продіагностувати віддалену систему та виявити її можливі слабкі місця, а також здійснити мережеву атаку в лоб, через шлюз в Інтернет або за допомогою ШПЗ, з'явилися [42]:

- комплексні атаки, які здійснюються через кілька векторів атак, не викликаючи підозр у вищеописаних систем кіберзахисту;
- різні варіанти прихованих шкідливих програм, у тому числі безфайлове ШПЗ, що проникає через поштові системи та Web-сесії, що маскуються в зображеннях, та ін.

Тому сучасна КСІК повинна містити компоненти, що виконують різні функції і доповнюють один одного, зокрема:

- захист мережевого рівня;
- захист робочих станцій та серверів;
- захист даних, що зберігаються та обробляються в КІС;
- аналітичні системи кібербезпеки.

До систем захисту мережевого рівня належать:

- ММЕ наступного покоління (NGFW);
- мікросегментація, у тому числі у віртуальній інфраструктурі;
- системи керування доступом до мережі (NAC);
- віддалений доступ із нульовою довірою (ZTNA);
- системи захисту від розподілених атак типу «відмова в обслуговуванні» (DDoS);
- системи захисту від атак на портали (WAF);
- брокери безпечного доступу до хмар (CASB.)

До систем захисту робочих станцій та серверів належать:

- системи захисту від ШПЗ, у тому числі від невідомого раніше;
- система захисту від атак через електронну пошту;
- система керування мобільними пристроями (EMM/MDM);
- система управління ідентифікацією, авторизацією користувачів та обліковими записами (IAM);
- система керування привілейованим доступом;
- системи захисту фізичного доступу.

До систем захисту даних відносять:

- системи захисту від витоку інформації (DLP);
- система багатофакторної аутентифікації та авторизації (MFA);
- системи резервного копіювання та відновлення й системи архівації;
- системи захисту БД.

До аналітичних систем кібербезпеки належать:

- система аналізу вразливостей;
- система імітації атак;
- система кіберпасток;
- система збирання, кореляції та аналізу журналів та дій (SIEM);
- система автоматизації дій під час розслідування чи реакції на інцидент.

Окремо хотілося б зазначити, що часто ставлять рівність між кібер- та інформаційною безпекою. Це не зовсім правильно. Інформаційна безпека займається забезпеченням безпеки даних, а саме: забезпеченням доступності авторизованим користувачам, захистом від неавторизованого доступу, захистом від знищення, захистом від спотворення тощо, у результаті будь-яких дій (кіберінциденту або виходу з ладу обладнання, або програмного збою, або відключення живлення, або руйнування каналів зв'язку та ін.). Кібербезпека, у свою чергу, захищає ІТ-інфраструктуру та дані від кібератак.

Надалі буде розглянуто системи кібербезпеки, куди не входять системи резервного копіювання та архівації інформації. Під словом «безпека» будемо мати на увазі саме кібербезпеку.

5.3.2. Корпоративні системи кібербезпеки

ММЕ наступного покоління (NGFW). Як випливає з назви, це пристрій перевірки і фільтрації трафіку, але, на відміну від своїх попередників, аналіз трафіку виконується на всіх рівнях моделі OSI аж до сьомого (Application layer), крім безпосередньо функцій ММЕ; є також функціонал системи захисту від вторгнень (IPS) та бази даних відомих шкідливих активностей і ресурсів, що оновлюється.

Таким чином, ММЕ наступного покоління аналізує та фільтрує трафік, використовуючи інформацію про IP-адреси, порти та ін. аж до додатку, якому належить кожен інформаційний потік. Рішення приймається інтелектуальним двигуном системи на підставі актуальної бази знань.

Такі пристрої встановлюють не лише на периметрі мережі, де вони виконують функцію шлюзів безпеки (Security Gateways, SWG), а й усередині КІС для контролю трафіку між сегментами та між вузлами КІС. NGFW можуть бути як апаратними, так і віртуальними, зокрема, працювати на рівні гіпервізора системи віртуалізації контролю трафіку безпосередньо між віртуальними машинами. Необхідність установлення NGFW всередині мережі та всередині вузлів аж до рівня віртуальних машин викликана необхідністю гранульовано розділяти та контролювати трафік для детекції шкідливої активності на ранньому етапі та запобігання розповсюдженню її по мережі. Таке саме завдання вирішує і мікросегментація.

Мікросегментація. Мережева технологія, що дозволяє поділити КІС на мінімально можливі логічні мережі, які передають окремі робочі навантаження, і не змішувати трафік, а також контролювати переміщення трафіку між цими логічними мережами, називається мікросегментацією. І що менші сегменти – то вища швидкість реакції на атаку і нижча швидкість її поширення по ІТ-інфраструктурі КІС. На нижчих рівнях моделі OSI можна використовувати, зокрема, і VLAN, але як один із механізмів, адже технологія мікросегментації динамічно налаштовується та функціонує і на другому та третьому рівнях моделі OSI, а у віртуальному середовищі – на рівні гіпервізора та віртуальних комутаторів.

Системи керування доступом до мережі (Network Access Control, NAC). Крім завдання поділу та фільтрації трафіку в КІС, стоїть ще завдання визначення та поділу користувачів, які намагаються підключитися до КІС на рівні мережі. Це завдання вирішується за допомогою протоколу IEEE 802.1x, при цьому система контролю та управління доступом до мережі має вміти визначати, як «хто» підключається до мережі за його ідентифікаторами, так і «що» підключається, тобто який пристрій. Визначення пристрою (тобто його профілювання) виконується не лише на базі MAC-адреси (Media Access Control) його мережевого адаптера, але також і за рахунок інших параметрів, оскільки підстановка «коректної» MAC-адреси стала вже повсякденною практикою, і без детального аналізу робоча станція зловмисника може постати перед камерою або сканером із доступом до серверного сегменту.

Після відповіді на запитання «хто?» і «що?» система приймає рішення «що робити?», а саме – чи надавати доступ і, якщо надавати, куди та з якими правами. Природно, що можливість профілювати пристрій, визначати, яке ПЗ встановлено, його версію та налаштування виходить повніше за наявності встановленого на цій робочій станції клієнтського ПЗ системи NAC, яка в разі корпоративних робочих станцій / ноутбуків установлюється разом з іншим ПЗ.

Віддалений доступ із нульовою довірою (Zero Trust Network Access, ZTNA). Різке зростання кількості працівників, які працюють віддалено і потребують підключення до інформаційних ресурсів КІС, призвело до двох результатів:

- класичний периметр організації ще більше розмився, і зросла роль інших засобів безпеки,
- важливість системи безпечного, зручного та функціонального віддаленого доступу до ресурсів КІС різко зросла.

Класична організація віддаленого доступу за допомогою IPSec VPN часто є незручною і вимагає великої кількості додаткових систем безпеки наближення до рівня контролю співробітників усередині периметра, адже в класичному вигляді вкрай складно контролювати ПЗ, встановлене на віддаленому ПК, його захист від Інтернету та ін.

Упровадження технології / рішення ZTNA дозволяє організовувати безпечне підключення до ресурсу або додатку КІС за рахунок автоматичної побудови шифрованого тунелю або тунелів до ресурсу або додатку, контролю наявності, версії та функціональності ПЗ або налаштувань на віддаленій робочій станції.

Найчастіше рішення реалізовано на проміжному шлюзі, який проводить аутентифікацію / авторизацію та перевірку робочої станції та користувача, а також визначає можливість підключення до тих чи інших ресурсів. Ефективні рішення даного класу мають можливість періодично, у рамках сесії, контролювати виконання умов допуску до ресурсів та змінювати авторизацію в разі, якщо умови перестали виконуватись – процедура Change of Authorization (CoA).

Дане рішення функціонально дуже схоже на розглянуту раніше систему управління доступом до мережі (NAC), але контролює віддалений доступ до ресурсів КІС і працює на інших протоколах та інших технічних реалізаціях.

Системи захисту від розподілених атак типу «відмова в обслуговуванні» (DDoS). Однією з найпоширеніших атак наразі є атака типу відмова в обслуговуванні. Н сьогодні в основному зустрічається розподілена версія атаки, яка здійснюється з тисяч IP-адрес. Суть атаки – у спробі перевищити пропускну здатність каналу, продуктивність шлюзу, продуктивність IT-систем (серверів, СЗД тощо) за рахунок генерування, зазвичай із багатьох джерел, великої кількості трафіку у вигляді хибних запитів, сміттєвих даних або спеціальних пакетів, що змушують витрачати на їхню обробку надмірну продуктивність. Для розуміння можливостей таких атак можна сказати, що в 2023 році на Google була здійснена атака обсягом 298 млн запитів за секунду, що більше, ніж кількість запитів до Wikipedia за весь вересень 2023 року.

Незважаючи на те, що автори таких атак бувають дуже винахідливими в способах обходу захисту, більшість атак є досить простими, їх дешево організувати, і вони просто генерують велику кількість сміттєвих даних у спробі переповнити канал даних, процесор шлюзу або MME. Якщо КІС для успішного функціонування необхідний доступ до зовнішніх ресурсів в Інтернет / хмарі або навпаки доступ зовнішніх користувачів до ресурсів КІС, а також якщо об'єднання вузлів КІС відбувається за допомогою шифрованих тунелів в Інтернет, то DDoS-атаки можуть бути згубними для роботи КІС і для функціонування підприємства в цілому.

Крім цього, DDoS-атаки можуть перевантажувати деякі елементи захисту, що в деяких виробників може призводити до пропуску трафіку без контролю перевантаженого пристрою. Можливий також пропуск командою безпеки підозрілих подій унаслідок перемикання уваги на відображення атаки DDoS.

Ураховуючи це, захист від DDoS-атак є дуже актуальним завданням і вирішується як на рівні хмарних центрів очищення, так і на рівні сервісів операторів та локальних пристроїв захисту на периметрі КІС.

Системи захисту від атак на портали (WAF). Для забезпечення доступу зовнішніх користувачів до внутрішніх ресурсів КІС необхідно не лише забезпечити захист від DDoS, але й забезпечити захист самого frontend-порталу (по суті, WEB-додатку) від специфічних атак на WEB-інфраструктуру. Проблематикою захисту від таких атак займається проєкт OWASP (Open Web Application Security Project), відомий публікацією поточного переліку 10 найбільш актуальних способів атаки на WEB-додатки (OWASP Top 10). Захист від атак на WEB-додаток виконує WAF, який встановлюється в інфраструктуру КІС після системи захисту від DDoS, шлюзу в Інтернет, але перед WEB-додатком, що захищається.

Брокери безпечного доступу до хмар (Cloud Access Security Broker, CASB). Коли йдеться про інфраструктуру КІС, зазвичай приділяють увагу ресурсам усередині периметра мережі, але не завжди звертають увагу на ресурси, розташовані в «хмарі», сподіваючись, що їх захистить оператор хмарної інфраструктури, що не є правильним, особливо з урахуванням кількості та швидкості зростання даних та систем, розташованих у «хмарах», а також відсутності зобов'язань операторів захищати дані користувачів від кібератак будь-якого типу (до речі, про збереження «хмарних» даних теж повинен піклуватися та копіювати їхній власник, а не оператор, за рідкісним виключенням придбання сервісу резервування). Існує цілий клас систем захисту ресурсів у «хмарах». Найбільш відомий із них – брокер безпечного доступу, який контролює права користувача для підключення до мережевих ресурсів, виходячи з його аутентифікації та поведінкового аналізу, перевіряє безпеку додатка для користувача, забезпечує виявлення хмарних додатків КІС, їхній моніторинг та управління на своєму рівні. Для захисту від несанкціонованого доступу система може заблокувати користувача або запропонувати йому пройти ще одну перевірку (використовувати ще один фактор аутентифікації), якщо на підставі впроваджених алгоритмів уважатиме, що його поведінка є аномальною або шкідливою.

Ще однією функціональністю рішення є захист даних від загрози знищення або спотворення та від витоку даних (DLP). Таким чином, CASB, з одного боку, захищає корпоративні додатки та дані в «хмарі» від неавторизованого доступу та впливу на інформацію, а також від викрадення інформації, а з іншого боку – від шкідливого впливу на робочі станції користувачів, а через них і на всю інфраструктуру КІС у разі компрометації хмарних програм та сервісів.

Системи захисту від ШПЗ, у тому числі від невідомого раніше. Антивірусне програмне забезпечення з'явилося дуже давно (майже 40 років тому) і відтоді еволюціонувало разом з еволюцією ШПЗ. Важливість цієї системи кібербезпеки у складі комплексу безпеки КІС неможливо переоцінити. Це останній рубіж оборони, якщо всі попередні рубежі не впоралися, й атака досягла своєї мети – обчислювального пристрою з даними. Систему боротьби із ШПЗ на обчислювальних пристроях зараз представлено двома типами рішень – EDR (Endpoint Detection & Response) та XDR (eXtended Detection & Response).

Обидві системи забезпечують виявлення відомого ШПЗ із великою ймовірністю та використовують інтелектуальні методи аналізу поведінки, передбачення та перевірки в «пісочниці» досліджуваного ПЗ для виявлення невідомого раніше шкідливого коду. Крім цього, такі системи виконують дії, спрямовані на запобігання шкідливим діям та боротьбу зі ШПЗ. Перевагою сучасних систем є централізація управління детекцією та реакцією для того, щоб інформація (профіль / ознаки / ...) про вірус, виявлений на одній робочій станції, повідомлялася на агент антивірусного ПЗ на інших робочих станціях для своєчасного виявлення та знищення ШПЗ, коли і якщо він потрапить на цю робочу станцію.

Відмінність EDR від XDR полягає в тому, що XDR для виявлення атаки використовує інформацію, одержувану не лише від робочої станції, а й від мережевих пристроїв, систем кіберзахисту та відповідних баз знань. Необхідно зазначити, що єдиного формалізованого опису, переліку функцій і характеристик XDR зараз немає, і кожен виробник вкладає в цю абревіатуру своє значення і свій погляд.

Система захисту від атак через електронну пошту. Вважається, що зараз електронна пошта є найпоширенішим вектором атак, тобто в більшості випадків брамою кібератаки на КІС стає шкідливе посилання або файл, відкритий користувачем в електронному листі. Тому системи захисту електронної пошти від кібератак є одним із найважливіших компонентів кіберзахисту.

Система захисту електронної пошти полягає у:

- перевірці кожного листа на наявність вбудованих потенційно шкідливих експлойтів та їхньому блокуванні;
- блокуванні листів, отриманих із скомпрометованих або шкідливих доменів;
- видаленні / блокуванні посилань на шкідливі або підозрілі сайти;
- видаленні з листа шкідливих файлів та файлів налаштованого типу / розширення;

• передаванні до карантину / «пісочниці» підозрілих вкладень або вкладень із певними ознаками;

• попередженні про підозрілий формат, структуру або список адресатів.

Цей функціонал побудований на передбачених правилах обробки з можливістю їх кастомізувати та доповнювати командою безпеки КІС із використанням оновлюваних баз знань шкідливих та підозрілих доменів, адрес, структур листа та хешей вкладень. Можливість перевіряти виконувані та офісні файли в «пісочниці» для виявлення потенційно шкідливої поведінки також є потужним інструментом захисту, поряд з інтелектуальним двигуном самого інструментарію.

Ще одним рівнем захисту електронної пошти, можливо, найголовнішим, є навчання всіх користувачів основам кібербезпеки при роботі з електронною поштою (часто називають – кібергігієні) і періодичне тестування їхньої поведінки.

Система керування мобільними пристроями (Enterprise Mobility Management / Mobile Device Management, EMM/MDM). Захист мобільних пристроїв, які мають доступ до корпоративних даних, від злому або несанкціонованого доступу до інформації, з урахуванням різних способів використання, архітектури та ОС, потребує окремих підходів та окремого рішення.

На мобільний пристрій встановлюється клієнтське ПЗ системи EMM/MDM, яке створює шифровану область пам'яті, куди записуються корпоративні програми та дані, доступ до яких здійснюється відповідно до корпоративної політики, установлюється шифрований тунель у корпоративну мережу, за яким відбувається обмін даними та працюють усі корпоративні програми.

Система EMM/MDM відстежує актуальність версії ОС мобільного пристрою та антивірусного ПЗ та контролює налаштування безпеки мобільного пристрою. У разі втрати / крадіжки мобільного пристрою розшифрувати корпоративні дані на мобільному пристрої буде дуже важко, якщо не неможливо. Крім того, адміністратор генерує команду на видалення всіх даних корпоративної області та права доступу в корпоративну мережу з пристрою та з бази користувачів КІС.

Система керування обліковими записами та авторизацією користувачів (IAM). Однією з можливостей отримати неавторизований доступ до ІТ-ресурсів КІС є відсутність контролю за життєвим циклом облікових записів та за фактом й історією призначення чи позбавлення прав доступу конкретного співробітника до конкретної системи з конкретними

правами. Якщо кількість співробітників обчислюється десятками і немає високої плинності кадрів, то теоретично акуратний адміністратор або співробітник відділу кібербезпеки може вести такий журнал, наприклад, в офісному додатку. Але якщо кількість співробітників / облікових записів обчислюється сотнями і тисячами та/або наявна висока плинність кадрів, то без спеціальної системи управління обліковими записами та доступом існує дуже велика ймовірність неврахованих та непотрібних прав на доступ до систем та/або активних облікових записів звільнених або переведених співробітників.

Принцип роботи IAM полягає в тому, що IT-системи при спробі користувача до них підключитися, для підтвердження прав користувача на роботу з ними, звертаються до IAM, яка зберігає в собі всі права користувача для роботи з усіма IT-системами компанії, історію їхніх змін і хто дозволив зміни. Створення облікового запису зі стандартними правами для конкретного підрозділу та посади, зміна прав при переведенні співробітника до іншого підрозділу, а також видалення облікового запису відбуваються автоматично на підставі запису в ПЗ відділу кадрів. Для цього система IAM глибоко інтегрується із системою обліку персоналу (відділ кадрів), із системою управління підприємством (Enterprise Resource Planning, ERP) та з корпоративними IT-системами.

Система керування привілейованим доступом (PAM). З погляду маніпулювання даними та IT-системами, і навіть видалення слідів впливу, системний адміністратор є неконтрольованим тому, що має максимум привілеїв для роботи із системою. Вирішення цієї проблеми покладено на систему, яка може контролювати дії адміністратора та тримати його активності під наглядом команди кібербезпеки та його керівництва.

Особливість системи PAM полягає в тому, що її адмініструє команда безпеки, і системні адміністратори не мають доступу до її файлів, налаштувань та журналу подій, тобто не можуть впливати на неї. Системи цього класу побудовані як проксі-шлюз для доступу до адміністрування будь-якої IT-системи. Адміністратори мають права на доступ до системи PAM, але не мають доступу до цільових систем. Після підключення до PAM вони запитують доступ до цільових IT-систем й отримують його після узгодження відповідно до налаштованих правил та ланцюжка авторизації (офіцер безпеки, керівник, запити на уточнення мети тощо).

Під час сесії всі дії адміністратора контролюються та зберігаються в кількох форматах аж до відео з метою використання в подальшому розслідуванні. При цьому можливе негайне реагування (припинення сесії, повідомлення тощо) на задані команди або дії. Наприклад, спроба

введення команди на видалення БД або руйнування кластера тощо призведе до блокування сесії та запиту на команду безпеки та керівника.

Системи захисту фізичного доступу. Особливість комплексних систем безпеки полягає в тому, що, з одного боку, кібернетична інфраструктура захищається системами контролю фізичного доступу від неавторизованого доступу до IT-обладнання для його фізичного руйнування або для підключення до локальної консолі систем, яка вважається захищеною та надає набагато більше прав на маніпуляцію із системами, ніж через віддалений доступ. А з іншого боку, кіберзахист не дозволяє зловмиснику отримати доступ до систем фізичного захисту (контроль фізичного доступу або відеоспостереження) та внести на них зміни для отримання неправомірної авторизації на фізичний доступ до приміщень КІС.

До систем захисту фізичного доступу відносять:

- різні системи сигналізації на території та в приміщеннях;
- системи контролю та управління фізичним доступом, заснованим на різних способах авторизації та їхніх комбінаціях (ключ-токен, біометрія (відбиток пальця, малюнок вен, сітківка та ін.), пароль / код);
- системи відеоспостереження з функціями відеоаналітики, розпізнавання та пошуку;
- ситуаційні центри з функцій аналітики комплексних подій та реакції на них.

Системи захисту від витоку інформації (DLP). Витік даних можливий не лише внаслідок кібератак та отримання зловмисниками неавторизованого доступу до даних, а й унаслідок навмисного чи випадкового поширення чутливих даних співробітниками організації. Боротися із цією проблемою покликана DLP-система.

DLP може мати мережевий та хостовий модулі, які борються з витоками даних на відповідних елементах інфраструктури. Робота системи DLP ґрунтується на класифікації інформації / даних / файлів. Способи класифікації можуть бути побудовані на базі міток у файлах, метаданих, розширення файлів, розташування файлів, входження слів у файл тощо, а також класифікація вручну власником інформації або уповноваженою особою.

Сучасні системи DLP можуть попереджати про спробу несанкціонованого поширення інформації, запитувати причини такої спроби для прийняття рішення співробітником безпеки / керівником про дозвіл на цю активність або блокування таких спроб залежно від налаштувань, рівня допуску / дозволу співробітника та ступеня чутливості інформації, але в будь-якому разі інформація про таку спробу зберігається в журналах системи для можливості аналізу в подальшому.

Найкращі зразки систем DLP запобігають витоку багатьма можливими каналами (реального захисту немає лише від переписування з екрану на листок і фотографування з екрану не на корпоративний телефон, але це також може бути визначено системою аналітики відеоспостереження, якщо воно розгорнуте в робочій зоні). Серед очевидних та неочевидних каналів витоку: електронна пошта, знімні накопичувачі, мережеві та хмарні файлові архіви, соціальні мережі, месенджери, перетворення на зображення, копіювання інформації з файлу на файл або інше місце, роздруківка та ін.

При цьому спрацювання системи DLP далеко не завжди говорить про злий намір, в абсолютній більшості випадків – це ненавмисне порушення політик співробітниками, що ще раз підтверджує необхідність навчання співробітників основ кібергігієни.

Система багатофакторної аутентифікації та авторизації. Для зловмисника однією з найпривабливіших для злому систем на етапі Exploitation / Privilege Escalation послідовності етапів атак Kill Chain є отримання параметрів доступу до важливих робочих станцій чи систем. Отримання будь-яким способом (клавіатурний шпигун, соціальна інженерія, фішинг тощо) імені та пароля дозволяє проникнути всередину КІС і поширюватися до цільових систем.

Найпростішим способом перешкодити отриманню доступу до ресурсу мережі таким чином є використання багатофакторної аутентифікації (MFA), яка передбачає для користувача необхідність пройти аутентифікацію кілька разів, використовуючи різні способи / фактори (комбінація імені та пароля, біометрія, одноразовий згенерований пароль (OTP), USB-ключ, ін.). Така система захищає від компрометації одного способу доступу: наприклад, від неавторизованого використання USB-ключа зловмисником або підглянутого пароля. Багатофакторна аутентифікація робить можливість неавторизованого доступу набагато менш ймовірним і різко підвищує надійність аутентифікації та авторизації.

Системи захисту БД. Практично у 100 % атак метою та найбільшою привабливістю для зловмисників є інформація КІС. У більшості випадків побудови централізованої моделі КІС, корпоративні дані зберігаються у відмовостійкому територіально-розподіленому кластері БД. Саме тому отримання доступу до даних, які розташовані в БД, або їх знищення є реальною метою атаки. Це може бути виконано одним із розглянутих вище способів: через вразливі робочі станції та сервери, за допомогою привілейованих облікових записів, через помилки та вразливості в порталі та інше, а може бути використаний безпосередньо доступ

до БД з урахуванням її особливості. Тому окремо стоїть завдання захисту саме систем управління базами даних (СУБД) з урахуванням їхніх уразливостей, особливостей реалізації та доступу.

Функціями систем захисту БД є:

- прецизійне управління доступами до тих чи інших елементів БД або загалом до БД для реалізації моделі рольового доступу користувачів у рамках рекомендацій та законів про захист приватної, медичної та іншої інформації;
- управління доступами адміністраторів БД лише до БД у зоні його відповідальності;
- контроль коректності, цілісності конфігурації БД та управління її змінами;
- контроль оновлень СУБД;
- аудит дій користувачів / додатків та занесення їх до журналу подій;
- виявлення аномальних активностей у БД та повідомлення про них команду безпеки та/або блокування таких дій, користувачів або програм.

Система аналізу вразливостей. Досвідчений адміністратор та співробітник команди безпеки розуміє, що всі реалізації програмно-апаратних рішень мають свої особливості, свої тонкі місця та вразливості, якими може скористатися досвідчений зловмисник для виконання атаки. Одні вразливості «закриваються» виробником рішення черговими оновленнями ПЗ; інші вразливості мають рекомендації стосовно заходів щодо запобігання їх використанню; треті вразливості поки що не мають ні таких оновлень, ні рекомендацій – вони просто відомі. Крім того, існують вразливості, для використання яких зловмисники вже розробили ШПЗ, та вразливості, для яких поки що таке ПЗ не випустили або поки що такою вразливістю неможливо або вкрай складно скористатися.

Системи аналізу вразливостей якраз і проводять (періодично або постійно) сканування інфраструктури на виявлення таких відомих вразливостей із наданням звіту за результатами, у якому вказується вразливість, знайдена в конкретному елементі КІС, рекомендації щодо усунення цієї вразливості. Кожній знайденій вразливості надається рейтинг залежно від серйозності наслідків її експлуатації та можливості її скористатися для того, щоб команда безпеки пріоритизувала роботи з усунення даних уразливостей, а за неможливості усунути вразливість – купірувала її за допомогою інших систем.

Система імітації атак. Команді безпеки необхідно розуміти, наскільки вжиті дії та зусилля захистили інфраструктуру КІС від атак та проникнення. Чи все враховано і чи всі проломи та вразливості закриті (наскільки це можливо). Для цього виконують процедуру «тест на проникнення» (penetration testing), що виконується командою, яка виконує роль атакуючого зловмисника (red team). Ця команда може складатися як із фахівців самого підприємства (якщо вони мають відповідну компетенцію), так і із зовнішніх спеціалістів у цій галузі.

Цей тест виконується періодично, раз на рік або раз на пів року. У решту часу команда кібербезпеки підприємства сподівається, що тест був виконаний професійно і що в них усе добре, і ніякі нові проломи / вразливості не з'явилися. Альтернативою такого періодичного тестування є використання системи імітації атак (Breach and Attack Simulation, BAS), яка налаштовується на ІТ-ландшафт КІС і запускає набір атак для всіх існуючих у КІС ІТ-систем та систем кібербезпеки, а також імітацію атак, розрахованих на слабку ланку захисту – користувача.

Такі симуляції атак можуть запускатися так часто, як це може бути ефективно для даної інфраструктури в автоматичному або автоматизованому режимі. Команда безпеки вивчає підготовлені звіти з рекомендаціями щодо усунення знайдених «дір» у захисті та виконує «роботу над помилками» з наступним перезапуском симуляції атаки для підтвердження успішного виправлення знайдених проблем.

Система кіберпасток. Існує статистика, що в середньому з моменту проникнення зловмисників в ІТ-інфраструктуру підприємства до ідентифікації самого факту проникнення проходить понад 200 днів, а до моменту визначення, де і як сталося проникнення, ще більше 70 днів, причому за останні 5 років ці терміни принципово не змінювалися.

Найшвидше визначення факту вторгнення та скорочення терміну присутності зловмисників в ІТ-інфраструктурі для мінімізації збитків і втрат, якщо проникнення все ж таки вдалося, – основне завдання комплексу систем аналітики кібербезпеки. Одним із найефективніших засобів виявлення злому є системи кіберпасток (Deception, Honeypot тощо). Принцип дії цих систем полягає у створенні фіктивних корпоративних ІТ-ресурсів, вкрай привабливих для зловмисника (каталог AD, БД, поштові сервери, системи управління організацією, бухгалтерські програми тощо), які мають усі ознаки реальних систем, створюють той самий профіль трафіку, мають ті самі відкриті порти, але при цьому дають можливість себе виявити і підключитися. Факт спроби підключення, а також поведінки після підключення (фіктивний ресурс на відміну від справж-

нього можна легко виявити в інфраструктурі, і він недовго чинить опір злому) сигналізує про те, що в інфраструктуру проник зловмисник. З його поведінки можна зробити висновки про цілі та спосіб проникнення для того, щоб підготуватися до захисту реальних ресурсів й убезпечити дані та постаратися виявити фізично зловмисника, поки він розбирається з фіктивною інформацією на фіктивному ресурсі.

Система збирання, кореляції та аналізу журналів і дій (SIEM). Для того щоб ідентифікувати спробу злому або шкідливу активність зловмисника в ІТ-інфраструктурі КІС, необхідно мати повну видимість усіх процесів у КІС. Для цього необхідно зібрати та проаналізувати багато тисяч записів у журналах подій, події безпеки та велику кількість іншої інформації. У результаті кореляції даних від багатьох ІТ-систем та систем кібербезпеки може бути виявлений кіберінцидент. Уважається, що лише таким чином можна виявити сучасні багатовекторні цільові атаки, спеціально розроблені для атаки на дану інфраструктуру. Саме такі атаки прийнято називати цільовою постійною загрозою підвищеної складності (Advanced persistent threat, APT), що несуть найбільшу загрозу.

Нездатність реальної команди кібербезпеки підприємства обробити, проаналізувати та прокорелювати десятки тисяч подій та записів на день призвела до появи SIEM-системи автоматичного збирання, аналізу та кореляції подій в інфраструктурі, завданням якої є автоматичне збирання подій у системі та аналіз за налаштованими правилами для виявлення потенційного інциденту безпеки та передання інформації про нього команді безпеки для проведення розслідувань, прийняття рішення про наявність інциденту та реакції на нього. У періоди між цілеспрямованими масованими атаками на організацію таких інцидентів у середній організації з'являється 2–5 на день, що вже реально розслідувати силами кваліфікованої команди безпеки.

Система автоматизації дій під час розслідування чи реакції на інцидент. У розслідуванні інциденту та реакції на нього важливим є запобігання або зменшення шкоди від атаки, а отже, мінімізація часу присутності зловмисників в інфраструктурі КІС, адже поки команда безпеки ідентифікує та локалізує присутність зловмисника в ІТ, зловмисник продовжує шкідливі дії. У процесі розслідування та реакції на інцидент дуже багато дій є рутинними та характерними для тієї чи іншої атаки чи активності. Наприклад, такими діями під час розслідування є: з'ясування атакуючих IP-адрес, країни, історії появи та досвіду боротьби, схожих атак на цей же ресурс тощо; а для реакції: блокування даної IP-адреси

або поштового домену; видалення або блокування активного контенту та вкладень у всіх листах із даного поштового домену; відправлення файлів, що відповідають ряду ознак, на перевірку в «пісочницю»; відключення від мережі даної робочої станції; блокування або зниження прав доступу для скомпрометованого облікового запису; запуск відповідних додатків та інші. Кожна команда безпеки сама формує послідовність дій, характерних для тієї чи іншої ситуації.

Виконання даних дій автоматично або автоматизовано за командою оператора або спрацьовування тригера появи того чи іншого інциденту дозволяє економити десятки й сотні хвилин у найбільш напруженій стадії розслідування та реакції, що може істотно знизити ту шкоду, якої завдає зловмисник.

Автоматизацію процесів у кібербезпеці здійснюють системи класу SOAR (Security orchestration, automation and response), які мають велику кількість вбудованих послідовностей дій для більшості стандартних ситуацій, дозволяють налаштовувати та створювати нові послідовності дій. Створення нового набору команд / дій може виконати спеціаліст безпеки без навичок програмування у графічному інтерфейсі, методом перетягування у правильне місце на схемі відповідних піктограм дій та стрілок умовних та безумовних переходів.

Для ефективної взаємодії з IT-інфраструктурою та системами безпеки SOAR мають вбудовану інтеграцію з абсолютною більшістю існуючих IT-систем та систем кібербезпеки, які дозволяють SOAR отримувати додаткову інформацію для збагачення події та виконання необхідних дій. Крім того, якщо такої інтеграції немає, то SOAR дозволяє створювати інтерфейси до третіх систем на основі вбудованого інструментарію.

5.3.3. Архітектура КСІК

Перераховані вище системи безпеки створюють екосистему корпоративної безпеки у складі чотирьох згаданих кластерів: безпека робочих станцій, безпека даних, мережева безпека та аналітика. Вибір необхідних систем кіберзахисту для побудови КСІК визначається на етапі проєктування з урахуванням IT-ландшафту, структури корпоративної мережі, критичності IT-ресурсів тощо [43].

У кожному конкретному випадку склад КІСК може відрізнятися залежно від наявності та важливості тієї чи іншої IT-системи. Наприклад, якщо немає порталу або його функціональність некритична – необхідність WAF сумнівна.

Принципово важливими компонентами є рішення щодо захисту мережі типу NGFW, захист робочих станцій і серверів від ШПЗ на базі EDR/XDR, захист системи електронної пошти. Украй рекомендованими компонентами також є: система управління доступом до мережі (NAC) та віддаленим доступом із нульовою довірою (ZTNA), захист від витоків інформації, комплекс систем аутентифікації та авторизації.

Рішення про доцільність використання інших систем кібербезпеки залежить від наявності відповідних IT-систем в організації, які потрібно захищати даною технологією кіберзахисту. При цьому для організацій середнього та великого розміру або із середньою чи високою складністю IT-ландшафту системи кластера аналітики кібербезпеки є критично важливими, особливо системи збирання та кореляції подій та система аналізу вразливостей. Така увага системам аналітики приділяється насамперед унаслідок того, що багато сучасних атак можна виявити лише в результаті аналізу подій у кількох системах, при цьому кожна така подія буде в гіршому випадку підозрілою, але не викличе реакції спеціалізованої системи кіберзахисту – фаєрволу, захисту кінцевої точки тощо. Лише сукупність цих подій може виявити факт здійснювання багатовекторної атаки. Також дуже рекомендованою до включення до складу КСІК є система кіберпасток і система оркестрації та автоматизації реакції. Ураховуючи вищевикладене, архітектура КСІК має бути такою (рис. 5.9).

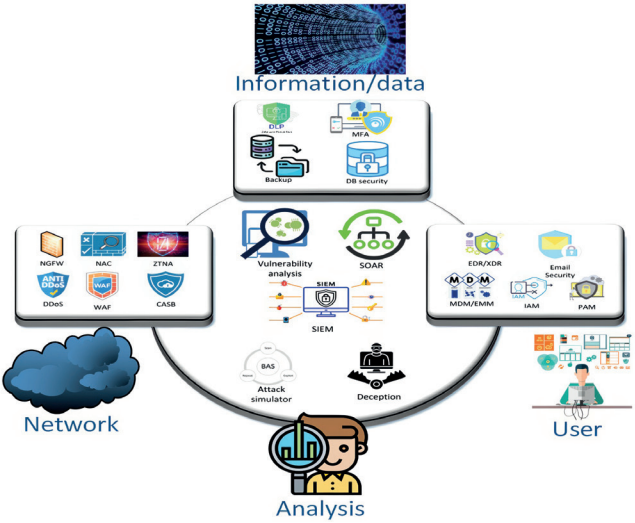

Рис. 5.9. Архітектура КСІК

Крім розглянутих технічних засобів захисту від кібератак, суттєва увага повинна приділятися навчанню співробітників та адміністраторів. Уважається, що до 40 % атак спрямовані на вразливість людини, так звана соціальна інженерія. Цей термін описує вивчення конкретної людини або групи людей для того, щоб зрозуміти їхню реакцію на запит, підготувати для них найбільш привабливе послання з тим, щоб вони стали точкою проникнення атаки в КІС.

Постійне навчання користувачів кібергігієні, тестування та робота над помилками можуть бути організовані в автоматизованому режимі за допомогою систем класу Security awareness training system, застосування яких може серйозно підвищити загальну кібербезпеку компанії. Крім того, існують спеціальні навчальні програми та полігони, які дозволяють підвищувати кваліфікацію та напрацьовувати досвід спеціалістам команди кіберзахисту та SOC.

Отже, сукупність описаних технологій кіберзахисту, правильний вибір необхідних систем захисту від специфічних загроз, побудова аналітичної платформи аналізу подій, пошуку загроз та реакцій на них, а також постійне навчання співробітників дозволить побудувати надійну ешелоновану систему ефективного кіберзахисту КІС.

5.4. Центр оперативного реагування на кіберінциденти

У сучасних умовах комп'ютеризації та інформатизації робота будь-якої організації тісно пов'язана із забезпеченням її інформаційної та кібербезпеки. Перед такими організаціями стоять завдання з оперативного збирання, обробки та аналітики інформації з метою якнайшвидшого реагування на події атак на ІТ-інфрастуктуру та усунення їх можливих негативних наслідків. Питання оперативного реагування на відхилення від штатної роботи ІТ-систем набувають особливої актуальності. Ефективна координація дій структурних підрозділів організації у випадку виникнення позаштатних ситуацій унаслідок кібератак вимагає формування центральної точки збирання інформації та аналітики для оперативного реагування на кіберінциденти з метою підтримки прийняття рішень. Усе це ставить додаткові завдання з контролю периметру ІТ-інфраструктури організації для забезпечення цілісності, конфіденційності, достовірності та доступності інформації, а також своєчасного запобігання втраті, витоку, крадіжці чи пошкодженню інформаційних активів організації. Тому питання створення і впровадження інструментальних засобів, що дають змогу ефективно

розв'язувати перераховані вище завдання, є досить актуальним. Як такий інструмент пропонується ЦОРК, що дозволяє ефективно забезпечити [44]:

- оперативну аналітику, спільну роботу та обмін даними;
- запис дзвінків, відеоконференцзв'язок та IP-телефонію;
- кореляцію та аналіз подій інформаційної та кібербезпеки;
- автоматизований пошук уразливостей ПЗ корпоративної IT-інфраструктури та апаратних засобів;
- підвищення швидкості реакції на події безпеки;
- підвищення ефективності аналізу та локалізації нештатних ситуацій, проблем у роботі критичної IT-інфраструктури;
- відстеження та оперативне усунення зловмисних дій зовнішніх факторів та/чи атак;
- шифрування даних, протидію витокам, управління інформаційною та кібербезпекою;
- безпечне підключення суміжних та підпорядкованих підрозділів до інфраструктури ЦОРК для спільної взаємодії та обміну даними між об'єктами та підрозділами IT-інфраструктури організації;
- відмовостійкість у випадках збою обладнання, інтернет-каналів зв'язку чи повного відключення об'єкта від мережі електроживлення.

Для створення ЦОРК використовується програмне та апаратне забезпечення таких виробників, як: Microsoft, Fortinet, Tenable, ESET, Cisco Systems, Samsung. Складові ЦОРК (наведено на рис. 5.10):

- система «відеостіна» та управляюче ПЗ;
- типове робоче місце оператора / фахівця;
- програмно-апаратне забезпечення збирання, аналітики, сканування та контроль використання інформаційних ресурсів;
- системи протидії витокам інформації, контролю доступу до інформаційних ресурсів, автоматизовані системи пошуку вразливостей;
- серверне обладнання для обробки та зберігання даних, віртуальна інфраструктура;
- телекомунікаційна мережа, міжмережеві екрани, IP-телефонія, відеоконференцзв'язок, система обміну повідомленнями, електронна пошта;
- система контролю доступу, відеоспостереження та аналітики.

Побудова ЦОРК передбачає проведення таких робіт:

- обстеження поточної інфраструктури, проєктування оперативного центру, модернізація корпоративної IT-інфраструктури з урахуванням вимог оперативного центру;

- підготовка кабельної мережі, систем безперебійного та гарантованого електроживлення, систем кондиціонування;
- впровадження систем інформаційної та кібербезпеки, контролю доступу, відеоспостереження та аналітики;
- впровадження систем моніторингу та управління інфраструктурою;
- обладнання приміщень центру, укомплектування меблями та допоміжним офісним обладнанням;
- гарантійне та постгарантійне обслуговування, технічний супровід, навчання персоналу.

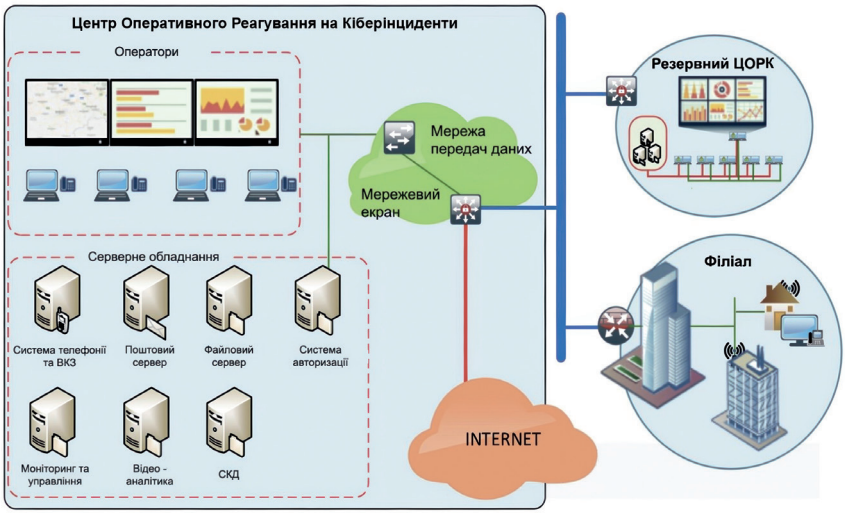

Рис. 5.10. Основні складові ЦОРК

Етапи та терміни впровадження: обстеження та проєктування – до двох місяців; постачання обладнання та ПЗ – від одного до трьох місяців; підготовка інженерної інфраструктури – від одного до двох місяців.

Таким чином, ЦОРК є ефективним інструментальним засобом забезпечення інформаційної та кібербезпеки організації, а загальна тривалість реалізації проєкту з його впровадження становить від трьох до шести місяців.

Висновки до п’ятого розділу

Проведено аналіз можливостей використання перспективних технологій у кібербезпеці, зокрема квантових, біометричних та ШІ. Розроблено операційну систему кібербезпеки, яка дозволяє забезпечити ефективний захист ІТ-інфраструктури організації від кібератак та кіберзагроз завдяки отриманню інформації про події та інциденти безпеки з різних джерел та проведенню їхнього кореляційного аналізу за допомогою ШІ. Також створено корпоративну систему інформаційної та кібербезпеки, яка забезпечує захист організації від великої кількості різноманітних загроз, безперервність процесів електронної обробки інформації, мінімізує ризики порушення їх функціонування та життєдіяльності.

Запропоновано інструментальний засіб протидії кіберзагрозам – центр оперативного реагування на кіберінциденти, який дає змогу ефективно забезпечити: оперативну аналітику, спільну роботу та обмін даними; запис дзвінків, відеоконференцзв’язок та IP-телефонію; кореляцію та аналіз подій інформаційної та кібербезпеки; автоматизований пошук уразливостей ПЗ корпоративної ІТ-інфраструктури та апаратних засобів; підвищення швидкості реакції на події безпеки; підвищення ефективності аналізу та локалізації нештатних ситуацій, проблем у роботі критичної ІТ-інфраструктури; відстеження та оперативне усунення зловмисних дій зовнішніх факторів та/чи атак; шифрування даних, протидію витокам, управління інформаційною та кібербезпекою; відмовостійкість у випадках збою обладнання, інтернет-каналів зв’язку чи повного відключення об’єкта від мережі електроживлення.

Перелік використаних джерел:

1. Виникнення штучного інтелекту : історія та сучасність (ШІ). URL: https://catsite.com.ua/vynyknennya-shtuchnogo-intelektu-istoriya-ta-suchasnist-shi/#google_vignette (дата звернення: 02.03.2024).

2. Turing A. M. Computing Machinery and Intelligence. *Mind.* 1950. № 49. С. 433–460.

3. Лисецький Ю. М., Сокур В. В. Теоретичні та математичні основи штучного інтелекту. *Вісник воєнної розвідки*. 2024. № 85. С. 51–56.

4. Лисецький Ю. М., Моркляник Б. В. Складові штучного інтелекту. *Вісник воєнної розвідки*. 2025. Спецвипуск «Штучний інтелект у сфері безпеки і оборони». С. 4–8.

5. Лисецький Ю. М. Основи та складові штучного інтелекту. *Military strategy and technology*. 2025. № 1 С. 76–80.

6. Сфери застосування штучного інтелекту. URL: https://aiconference.com.ua/uk/news/oblasti-primeneniya-iskusstvennogo-intellekta-92253 (дата звернення: 02.03.2024).

7. 17 прикладів застосування штучного інтелекту у повсякденному житті. URL: https://futurenow.com.ua/5-prykladiv-shtuchnogo-intelektu-u-shhodennomu-zhytti/#google_vignette (дата звернення: 02.03.2024).

8. Кармазіна М. С. Використання штучного інтелекту в освіті та науковому аналізі. *Вісник воєнної розвідки*. 2024. № 77. С. 83–87.

9. Кармазіна М. С. Виклики сьогодення: дезінформація в контексті розвитку штучного інтелекту та когнітивних воєн сучасності**.** *Вісник воєнної розвідки*. 2024. № 80. С.77–82.

10. Сокур В. В., Лисецький Ю. М., Паршуков С. С. Перспективи використання штучного інтелекту в сфері кіберрозвідки. *XXIII науково-методична конференція «Проблеми та перспективи підготовки фахівців воєнної розвідки в умовах відсічі російської воєнної агресії»,* 28 листопада 2024 року, м. Київ. Науковий збірник № 57. С. 100.

11. Лисецький Ю. М., Данченко О. І. Використання штучного інтелекту в сфері кібербезпеки. *Вісник воєнної розвідки*. 2025. № 86. С. 42–45.

12. Лисецький Ю. М., Короленко І. Г. Перспективні технології кіберзахисту на основі штучного інтелекту. *Міжвідомча науково-практична конференція «30 років ВА імені Євгенія Березняка: актуальні проблеми розвідки, контррозвідки, правоохоронної діяльності в умовах широкомасштабної збройної агресії рф проти України»*. 2 квітня 2024 року, м. Київ. Науковий збірник № 54. 115–117.

13. Вплив штучного інтелекту на сферу кібербезпеки. URL: https://softico.ua/uk/news/vpliv-shtuchnogo-intelektu-na-sferu-kiberbezpeki/ (дата звернення: 10.03.2024).

14. Кушіль Д. О., Лисецький Ю. М., Данченко О. І., Сурма А. І. Особливості використання технології штучного інтелекту у сфері кібербезпеки. *XXIII науково-методична конференція «Проблеми та перспективи підготовки фахівців воєнної розвідки в умовах відсічі російської воєнної агресії»,* 28 листопада 2024 року, м. Київ. Науковий збірник № 57. С. 82.

15. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. URL: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-

ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku (дата звернення: 10.03.2024).

16. Загрози та ризики використання штучного інтелекту. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/520 (дата звернення: 12.03.2024).

17. Квантові технології в обороні і безпеці. URL: https://www.nato.int/docu/review/uk/articles/2021/06/03/kvantov-tehnolog-v-oboron-bezpets/index.html (дата звернення: 14.01.2024).

18. Куцаєв В. В., Головко О. Є., Лазута Р. Г. Перспективи використання квантових технологій. *Вісник ВІТІ*. Комунікаційні та інформаційні системи. Випуск № 1 (3), 2022. С. 26–41.

19. Лисецький Ю. М., Боханченко О. С., Сурма А. І. Використання квантових технологій для забезпечення кіберзахисту. *Міжвідомча науково-практична конференція «30 років ВА імені Євгенія Березняка: актуальні проблеми розвідки, контррозвідки, правоохоронної діяльності в умовах широкомасштабної збройної агресії рф проти України»*. 2 квітня 2024 року, м. Київ. Науковий збірник № 54. С. 114–115.

20. V Сольвеевский конгресс. URL: https://postnauka.org/wtf/156386 (дата звернення: 20.03.2025 р.).

21. Лисецький Ю. М., Сурма А. І., Данченко О. І. Квантові технології. Нові можливості в кібербезпеці. *Вісник воєнної розвідки*. 2024. № 81. С. 44–47.

22. Квантові обчислення та кібербезпека: загрози та рішення. URL: http://surl.li/gvqgx (дата звернення: 12.01.2024).

23. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. – Львів : ЛьвДУВС, 2015. 492 с.

24. Іванова О. М. Біометричні технології у кіберзахисті**.** *Кібербезпека: освіта, наука, техніка*. 2020. № 61. С. 45–53.

25. Бідюк П. І., Бондарчук В. С. Сучасні методи біометричної ідентифікації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2009. № 1 (18). С. 137–146.

26. Петров В. І. Застосування біометричних систем у кіберзахисті інформації. *Інформаційні технології в освіті, науці і виробництві*. 2018. № 42. С. 112–120.

27. Сидоренко Л. П. Використання біометричних систем у захисті корпоративної інформації**.** *Інформаційна безпека і захист інформації*. 2019. № 79. С. 76–82.

28. Лисецький Ю. М., Данченко О. І. Використання біометричних технологій для підвищення рівня кібербезпеки. *Вісник воєнної розвідки*. 2024. № 83. С. 44–48.

29. Гриценко А. О. Роль біометричних технологій у підвищенні рівня кібербезпеки. *Кібернетика та комп'ютерна інженерія*. 2021. № 54. С. 28–35.

30. Ковальчук В. М. Сучасні тенденції використання біометричних технологій у кіберзахисті. *Інформаційна безпека та захист інформації*. 2017. № 73. С. 94–102.

31. The Role of Biometric Technology in Information Security. URL: https://www.researchgate.net/publication/279508922_The_Role_of_Biometric_Technology_in_Information_Security (дата звернення: 14.04.2024).

32. Biometrics and Security | Cybersecurity and Governance. URL: https://www.csis.org/programs/strategic-technologies-program/past-work/cybersecurity-and-governance/biometrics-and (дата звернення: 16.04.2024).

33. The Role of Biometrics in Cybersecurity: Threats and Solutions. URL:

34. Лисецький Ю. М., Енько М. В., Лабунець О. О. Використання біометричних технологій для підвищення рівня кібербезпеки. *XXIII науково-методична конференція «Проблеми та перспективи підготовки фахівців воєнної розвідки в умовах відсічі російської воєнної агресії»*, 28 листопада 2024 року, м. Київ. Науковий збірник № 57. С. 83.

35. Лисецький Ю. М., Бобров С. І. Security Operation Systems. *Математичні машини і системи.* 2020. № 2. С. 51–59.

36. ATT&CK for Enterprise Introduction URL: https://attack.mitre.org/resources/enterprise-introduction/ (дата звернення: 05.12.2023).

37. Лисецький Ю. М. Побудова операційної системи кібербезпеки з використанням штучного інтелекту. *Вісник воєнної розвідки*. 2025. Спецвипуск «Штучний інтелект у сфері безпеки і оборони». С. 50–56.

38. Лисецький Ю. М., Молдаван В. Т., Семібаламут К. М. Розробка архітектури операційної системи кібербезпеки. *Вісник воєнної розвідки*. 2024. № 78. С. 25–30.

39. Лисецький Ю. М., Бобров С. І., Данченко О. І. Корпоративна система інформаційної та кібербезпеки. *Математичні машини і системи*. 2024. № 3. С. 37–49.

40. Лисецкий Ю. М. Комплексная безопасность корпоративных информационных систем. *Управляющие машины и системы*. 2019. № 1. С. 68–75.

41. Лисецький Ю. М. Некоторые аспекты комплексной безопасности корпоративных сетей. V міжнар. наук.-практ. конф. *«Інформаційні управляючі системи та технології»* (Одеса, 20–22 вересня 2016 р.). – Одеса, 2016. – С. 145–148.

42. Міжмережевий екран: що це та як працює? URL: https://ukeywaf.com/baza/mizhmerezhevyj-ekran-shho-cze-yak-praczyuye/ (дата звернення: 10.01.2023).

43. Лисецький Ю. М. Розробка архітектури корпоративної системи кібербезпеки з використанням штучного інтелекту. *Вісник воєнної розвідки.* 2025. Спецвипуск «Штучний інтелект у сфері безпеки і оборони». С. 57–67.

44. Лисецький Ю. М. Центр реагування на інциденти інформаційної безпеки. *Сектор безпеки і оборони України; технології асиметричного протиборства:* наук. зб. № 42 матеріал. наук.-практ. конф. (м. Київ, 04 грудня 2020 р). Київ, 2020, С. 22.

ВИСНОВКИ

У монографії досліджено проблему забезпечення кібербезпеки держави. При цьому отримано такі теоретичні та практичні результати:

- наведено сутнісні характеристики формування механізму міжнародної кібербезпеки;
- запропоновано концептуальні засади державного регулювання у сфері інформаційно-комунікаційних технологій для забезпечення національної безпеки та концептуальні основи побудови системи національної кібербезпеки;
- розроблено модель системи національної кібербезпеки і модель взаємодії та обміну інформацією між центрами протидії кіберзагрозам;
- наведено існуючі підходи до забезпечення інформаційної та кібербезпеки, організаційно-технічні методи підвіщення рівня кіберзахисту інформаційних систем, способи організації безпеки корпоративних баз даних, особливості забезпечення інформаційної та кібербезпеки в корпоративній мережі при віддаленому доступі;
- запропоновано автоматизацію управління правами користувачів ІТ-систем як засіб підвищення ефективності інформаційної та кібербезпеки;
- досліджено проблему забезпечення кібербезпеки при використанні технології Інтернету речей і систем промислового Інтернету речей та розроблено рекомендації щодо кібербезахисту IoT-пристроїв;
- проведено аналіз можливостей використання перспективних технологій у кібербезпеці, зокрема квантових, біометричних та штучного інтелекту;
- розроблено корпоративну систему інформаційної та кібербезпеки, а також сучасні інструментальні засоби протидії кіберзагрозам – операційну систему кібербезпеки і центр оперативного реагування на кіберінциденти.

У цілому отримані результати у вигляді концептуальних засад, моделей, методів, технологій та засобів створюють методологічні та організаційно-технічні основи, що надають загальне бачення та розуміння можливостей для розвитку і вдосконалення системи національної кібербезпеки.

Наукове видання

Лисецкий Юрий Михайлович

КІБЕРБЕЗПЕКА: ВИКЛИКИ, ЗАГРОЗИ, ПРОТИДІЯ

Монографія

Літературний редактор, коректор – А. В. Галушкіна
Комп'ютерна верстка, макетування – В. Ю. Бихун
Дизайн обкладинки – О. О. Старовойтенко

Підп. до друку 06.02.2026. Формат 64x90/16.
Папір крейдований. Друк офсетний.
Ум. друк. арк. 13,11. Тираж 500 прим. Зам. № 01/2
Видавець Бихун В. Ю.
вул. Леонтовича, 9, к. 18, м. Київ, 01054
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції
ДК № 5366 від 26.06.2017 р.
тел./ факс: +38 044 235 75 28
моб.: +38 050 310 22 04
e-mail: lk@ukr.net