Науково-методичне видання

TRANSLATION FOR SPECIFIC PURPOSES

(Cybersecurity)

Навчальний посібник

В авторській редакції

Укладачі – *Пальчевська О.С., Маланюк М.С.*

Відповідальний за випуск – *Лук'яненко В.В.*

Підписано до друку 13.10.2021р.
Формат 60х 84/16. Друк числовий. Папір офсетний.
Гарнітура Times New Roman. Обл.-вид. арк. 10,97.
Ум. друк. арк. 12,32. Тираж 300 прим.
Зам. № 628.

Віддруковано з оригінал-макету замовника

Видавець - ФОП Лук'яненко В.В. ТПК «Орхідея»

*Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
серія ДК № 3020 від 02.11.2007 р.*

*16600, Чернігівська обл., м. Ніжин, вул. Небесної Сотні, 13 а.
Тел.: 098 815 06 60*
E-mail: holdingvv@ gmail.com

TRANSLATION FOR SPECIFIC PURPOSES

(Cybersecurity)

Навчальний посібник

Львів
2021

Рецензенти:

Аладько Д. О. – доцент кафедри романо-германської філології факультету іноземної філології Рівненського державного гуманітарного університету.

Ткачук Р.Л. – д. тех. наук, начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Рекомендовано до друку Вченою радою Навчально-наукового інституту психології та соціального захисту протокол № 3 від 17 червня 2021 року

Рекомендовано до друку Вченою радою ЛДУ БЖД
Протокол № 2 від 6 жовтня 2021 р.

TRANSLATION FOR SPECIFIC PURPOSES. Навчальний посібник. / Укладачі Пальчевська О.С., Маланюк М.С. Л., 2021. 212 с.

ISBN 978-617-7609-67-3

Навчальний посібник адресовано студентам, які вивчають курс «Галузевого перекладу» з англійської мови як першої іноземної. Мета посібника – формування у студентів перекладацької компетенції, а саме спеціальної складової її прагматичної частини, що передбачає знання, вміння та навики, які необхідні перекладачу при перекладі тестів у сфері кібербезпеки. Посібник містить необхідний практичний матеріал, що ґрунтується на теоретичних положеннях, які студенти опановують протягом вивчення курсів "Вступ до перекладознавства", "Теорія та практика перекладу".

УДК

ISBN 978-617-7609-67-3

Transmit – передавати сигнали;

Triggering – запуск;

Ubiquitous – універсальний, який зустрчається скрізь

Underpin – підтримувати, зміцнювати

User- data – дані користувача!

User-interface – інтерфейс користувача;

Vendor – продавець

Vicarious liability – відповіадльнсть за чужу провину

Vulnerability – слабка сторона;

Warrant – гарантія, патент, ордер

Web crawlers – пошуковий робот;

Without undue delay – без зайвого зволікання

Clear and convincing evidence – чітке і переконливе свідчення

Передмова

Сьогодні модель вищої освіти у галузі філології та перекладу реалізується з урахуванням сучасних суспільних реалій та потреб у висококваліфікованих перекладачах, коли визнається провідна роль мови для успішної міжкультурної комунікації та інтеграції України у світовий простір.

Для забезпечення ґрунтовних знань студентами у царинах лінгвістики та перекладу, динаміки та сучасних тенденцій у перекладознавчих практиках передбачається набуття як теоретичних так і практичних навичок галузевого перекладу.

Посібник «Translation for specific purposes (Cybersecurity)» інтегрує різні навчально-методичні матеріали, що допоможуть у підготовці фахівців-перекладачів у сфері кібербезпеки.

Матеріал підручника містить 21 розділ. У яких розглядаються основні положення забезпечення кібербезпеки на міжнародному, регіональному та національному рівнях. Проблемні питання забезпечення кібербезпеки на кожному з рівнів та шляхи їх вирішення. Особлива увага приділяється загрозам у сфері кібербезпеки та системі кібердій.

Посібник укладено у відповідності з новими освітньо-професійними програмами підготовки перекладачів. Він є базовим для формування різних аспектів перекладацької компетенції. Під час перекладу тексту сфери кібербезпеки доводиться вирішувати цілий комплекс різноманітних завдань. У посібнику такі тексти дібрані з огляду на лексико-граматичні особливості, насичесть термінами та спеціальною лексикою.

Метою посібника є формування та розвиток навичок письмового та усного перекладу з англійської мови на українську та з української на англійську, створення активного лексикону-мінімуму термінології сфери кібербезпеки. Досягнення поставленої мети забезпечує формування базових знань перекладача у галузі кібербезпеки.

Після успішного опанування поданого матеріалу студенти отримають знання про особливості та специфіку призначення текстів кібербезпеки; основний понятійний апарат таких текстів; положення щодо смислових та структурних особливостей термінологічної лексики сфери кібербезпеки; особливості етапів здійснення та редагування перекладу технічних текстів сфери кібербезпеки.

Матеріали для перекладу вміщені у посібнику дібрано з автентичних матеріалів нормативно-правового, навчального, довідкового та інформативного характеру (конвенції, стандарти, положення, інструкції, словники, довідники, енциклопедії, підручники, інтернет джерела) у сфері кібербезпеки. Список усіх використаних джерел подано в кінці посібника.

Relative ability – відносна здатність

Remedies – засіб, засіб захисту прав

Replication – тиражування;

Res ipsa loquitur – говорити по суті

Resilient – стійкий;

Safety property – властивості безперноьож

Scalable – масшбаний!

Search warrant – ордер на право обшуку

Selectively – вибірково;

Spoof – обдурити;

Stack – память;

Standard of Proof - необхідний ступінь доведеності

State - of -the -art – сучасний; attack – атака Сібілл ти як ,;

State of the art – на передовому рівні

Strict liability – пряма відповідальнсть

Subject matter – предмет вивчення

Substantive law – матеріальний закон, матеріальне право

Sui generis – за певної нагоди

Territorial jurisdiction – територіальна підсудність, територіальна юрисдикція

To take legal action – подавати до суду

Topology graphs – топологічна схема;

Tort – загальна система покарань за порушення правил цивільних норм

Tort liability – деліктне зобов'язання, відповідальність деліктна, відповідальність за шкоду

Tortfeasor – правопорушник

Tortious act – громадське правопорушення

Total cost – повна собівартість

Trade secrets – секрет професійної майстерності, методика

Trademarks – торгова марка

Trade-off – компроміс;

Notoriously – відомо;

Overlap – поєднувати операцій;

Overlay – організувати оверлейну програму

Patents - патенти та інші охоронні документи на об'єкти промислової власності

Penalties – санкції

Per se – в чистому вигляді

Personal data – особисті дані

Personal data breach - порушення правил захисту персональних даних

Perturbation – відхилення;

Piggybacked - поєднувати передачу прямих і зворотних пакетів;

Point-to-point – двох точкові;

Post-facto – після події

Preponderance of evidence – наявність більш вагомих доказів, перевага доказів

Prescriptive jurisdiction – приписова юрисдикція

Prima facie – при відсутності доказів на користь протилежного; оскільки не буде спростовано належними доказами; достатній за відсутності спростування; з першого погляду; перше враження

Privacy laws – закон про конфіденційність

Private key – секретний ключ;

Pro rata – пропорційний

Probable cause – наявність достатніх підстав

Proximate causation – слідчо-причинний зв'язок

Public domain – державна власність

Purpose limitation – цільове обмеження

Reasonable suspicion – обґрунтована підозра

Redirect – перенаправляти;

Reference monitor – контрольний індикатор;

Registries – регістратура, судова канцелярія

Regulatory system - система правового регулювання

CONTENTS

Unit 1. The scope of cybersecurity

I. Pre-reading activities.

Task 1. How do you understand the statement: "*As we've come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided.*" – Art Wittmann. **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What definitions of cybersecurity can you name?
2. What do you understand under the term digital information?
3. How do you think, are the terms safety and security the same? Why yes or no?

Task 3. Try to guess the meaning of the following words.

Hardware, software, launch, large-scale, maladaptation, chasing bugs, an adversarial environment, software breaches, implementation bug, remote control, remain bug.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1). Digital information ignores borders, and may even play with contradictions between the legislations of different countries or their 2). maladaptation to the digital age. 3). Software safety is concerned with the 4). absence of misbehavior, both in normal and exceptional situations, but still in a neutral environment when no one is trying 5). to intentionally attack the system. 6). Monitoring takes the form of 7). dynamic attack detection and 8). recovery mechanisms.

In rem – проти власності

Indicia – ознака

Information leak – злити інформацію;

Integrity – достовірність;

Intellectual property – об'єкт права інтелектуальної власності

Intrusion – вторгнення

Intrusion – проникнення;

Iris pattern – візерунок райдужної оболонки ока:

Jeopardise – ставити під загрозу

Juridical jurisdiction – судова юрисдикція

Jurisdiction – компетенція, сфера повноважень, судочинство

Lawful authority – законна влада

Ledger – програма фінансового звіту;

Legal action – судовий процес, звернення до суду

Legal causation – законна підстава

Legal risk – правовий ризик

Legislation – законодавство

Liability – обов'язок, необхідність

Licence fees – вартість ліцензії

Logging – введення даних;

Lookups – опитування;

Malicious – негативний;

Malware – програми, які порушують роботу системи

Middleware – міжплатформне програмне забезпечення;

Mitigation – вирішення проблеми;

Multilateral treaty – багатосторонній договір

National security – національна безпека

Negligence – необережність

Network partition – порушення зв'язку у мережі;

Non- trivial – нетривіальний;

Egregious violations – грубе порушення

Electronic interception – радіо перехват

Electronic surveillance – стеження з використанням радіоелектронних засобів

Employment disputes – сперечання пов'язані з трудовим правопорушенням

Encapsulate – формувати пакет даних;

Endpoint authentication –кінець ідентифікації;

Enforcement jurisdiction – виконавча юрисдикція

Entail – мається на увазі;

Entity – модуль, логічний об'єкт;

Enumeration – нумерація;

Exclusive rights – монопольне право

Exemplary damages - збитки, що присуджуються в порядку покарання

Expiry – закінчення терміну придатності;

Facet – сторона, грань;

Fair use – правомірне користування

Fall victim to – стати жертвою

Financial fraud – фінансовий обман, махінація

Foreseeability – передбаченість

Forfeiture of servers – втрата службового стажу

Gambling services – ігрові послуги

Habeas corpus - судовий наказ про доставляння арештованого в суд для з'ясування правомірності утримання його під вартою

Hack-back – обчислювальна техніка

Highly-scalable – великомасштабний;

Holistic approach – цілісний підхід, комплексний підхід

Human welfare – благополуччя людства

Illegitimate – визнати дитину, яка народилась поза шлюбом

Implication – співучасть;

Impose – всунути;

In absentia – за відсутності обох сторін, заочно

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1). database	a). домен
2). digital information	b). пульт дистанційного керування
3). software	c). динамічне виявлення атак
4). dynamic attack detection	d). цифрова інформація
5). remote control	e). база даних
6). domain	f). програмне забезпечення

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. Why physical security may depend on cybersecurity?
2. What is the first step to satisfy the safety property?
3. What are additional mechanisms based on dynamic error detection and recovery mechanisms used for?

The scope of cybersecurity

Wikipedia defines cybersecurity as follows: Computer security, also known as cyber security or IT security, is the protection of computer systems from the damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. However, the exact notion of cybersecurity differs depending on the context. Security in general includes both cybersecurity and physical security. However, cybersecurity requires some form of physical security, since physical access to computer systems enables a whole class of attacks. Conversely, physical security may depend on cybersecurity to the extent

that it uses computer systems, e.g., to monitor some physical space or maintain a database of authorized persons. Still, the difference between cyber- and physical security should always be clear, and we only address cybersecurity hereafter. Moreover, in many places, we will just use the word security to mean cybersecurity.

1. Physical security vs. cybersecurity.

Physical security and cybersecurity are quite different in nature. Digital information is immaterial: duplicating and exchanging data and code with anyone anywhere in the world is nowadays a trivial, extremely fast process, with almost zero cost. Hence, an attack or malware launched by a single person can spread worldwide, at a large-scale, in less than an hour. Digital information is of discrete nature: a single bit flip may introduce a critical failure and turn a perfectly working system into a malfunctioning one, which is then more vulnerable to compromise. This contrasts with the laws of physics, which tend to be continuous at a macroscopic level, and usually let one observe a slow deformation of a structure before it reaches its breaking point. Digital information ignores borders, and may even play with contradictions between the legislations of different countries or their maladaptation to the digital age. This makes cybersecurity much harder to achieve than other forms of security.

2. Safety vs. security.

Software safety is concerned with the absence of misbehavior, both in normal and exceptional situations, but still in a neutral environment when no one is trying to intentionally attack the system. Software safety is not just a matter of chasing bugs: it also calls for an analysis of the possible sources of misbehavior and how to handle them in a fail-safe manner. This requires a specification of the software's expected behavior, including a model of the environment, and some justification as to how or why the software respects its specification. In contrast, software security aims for the absence of misbehavior in an adversarial environment, where an attacker intentionally tries to misuse a system, putting it in an erroneous state that is not part of its intended specification. Security can also be

Contractual liability – відповідальність за договором

Coordination scheme – схема координації;

Copyright – копірайтинг, право інтелектуальної власності

Core feature – ключова особливість;

Corollary – слідство

Criminal liability – кримінальна відповідальність

Custodial sentences – покарання у вигляді позбавлення волі

Cyber security – кібербезпека

Cybercrime – кіберзлочин, комп'ютерний злочин

Data protection – охорона приватного життя громадян від зловживання інформацією

Database system – система баз даних

De minimis – в малій кількості

Decipherment – розшифрування

De-construct – деконструювати;

Dedicated entity – виділений модуль;

Defamation – наклеп

Denial- заперечення, спростування;

Discretionary – дискреційний;

Dissemination – передача сигналів;

Distributed system- система з функціями розподілення;

Domain – домен;

Domain names – позов про визнання незаконним використання товарного знака позивача в доменних іменах

Domestic law – внутрішнє право

Dual criminality – обопільне визнання, обопільне визнання відповідного діяння злочином

Duplicator – дублікатор;

Duty of care - обов'язок проявляти сумлінність

Eavesdropping – підслуховування;

пам'яті) без використання метаданих, що описують розташування та розташування артефактів. Різці даних використовують знання форматів даних для ідентифікації та перевірки витягнутого вмісту.

Caseworker – соціальний працівник;

Censorship – цензура:

Certificate – Структура даних з цифровим підписом, яка пов’язує сутність (звана темою) з деяким атрибутом.

Churn – перемішати;

Ciphertext – закодований текст

Civil judgment– слухання цивільної справи в суді

Civil liability – громадянська відповідальність

Click fraud – практика використання шкідливого програмного забезпечення для отримання підроблених кліків на веб-сайтах.

CMOS – комплементарна напівпровідникова технологія оксиду металу - найпопулярніша кремнієва технологія для створення інтегральних схем. Він складається з додаткових транзисторів PMOS та NMOS. Основними його перевагами є те, що він має дуже низьке споживання статичної енергії та відносно надійну роботу. Отже, це дозволило інтегрувати тривожну кількість транзисторів (від мільйонів до мільярдів) в одну інтегральну схему.

Collusion – таємний договір;

Competition law – законодавство про захист конкуренції

Compromise – Розголошення інформації сторонніми особами або порушення цієї політики безпеки системи, в якій могло статися несанкціоноване навмисне або ненавмисне розкриття, модифікація, знищення або втрата предмета.

Computational – машинний;

Computer crime – злочинне використання технічних можливостей комп'ютера

Conflict of law – колізія права

Consistency – послідовність, логічність;

approached by modeling the environment, but this is much harder to achieve exhaustively, because attackers do not comply with predefined rules, but rather continuously search for previously unknown means of attack. Hence, security also requires us to keep up-to-date with attackers’ progress in all areas (software breaches, algorithms and techniques, hardware capabilities, etc.). A complementary approach consists in describing normal execution paths and monitoring execution, so as to raise an alarm and react appropriately when some trajectory goes outside of normal executions.

3. Safety vs. security.

The terms security and safety are sometimes misused. Safety refers to accidental threats, due to internal misbehaviors or non-intentional misuse of the system, while security refers to intentional threats. Safety deals with fault-tolerance, while security deals with resistance to attacks. For example, a car may crash because of a software specification or an implementation bug (safety issues), or because of an attacker taking remote control of the vehicle (a security issue).

Despite these differences, safety and security are often tied to one another. Since security works in an adversarial mode, it should also consider accidental threats which may be exploited by the attacker. Hence, security is a stronger requirement than safety. In many situations, however, the software is exposed to the outside world, typically connected to the Internet, where attacks are the norm – and safety without security would often not make much sense! Safety and security also share a lot in their methodologies. Dealing with the safety of large software systems that interact with the physical world, such as Cyber-Physical Systems (often known as CPS), has led to some well established methodologies. One should start with a safety risk analysis phase, where all situations that may lead to catastrophic consequences are explored. Representations such as fault trees can be used to systematically describe such situations. The identified risks are then quantified to estimate the probability of the occurrences of these situations. Ensuring safety means ensuring that this probability remains below a given threshold. Of course, a first step to satisfy the safety property is to ensure the

absence of internal faults (bugs) in the software, as these faults are the primary cause of failures. Formally, one writes a software specification to describe the expected behavior of the software, and then shows that the actual implementation satisfies the specification. Unfortunately, not all cases may have been considered in the specification. Moreover, there may be external faults (for example, an erroneous value coming from an external sensor) that are not considered in the software specification, and that can lead to disasters. Hence, we must also use additional mechanisms, essentially based on dynamic error detection and recovery mechanisms, used to treat the errors due to external faults before they lead to catastrophic consequences. A similar approach applies to security. A security risk analysis replaces the safety risk analysis. While it is not possible to reason statistically to build an unassailable system in the case of security, it is still useful to ensure that there are no bugs (at least of some kind) in the software, for example by the same formal approach as the one followed for safety, because attacks often build on vulnerabilities that stem from a remaining bug. Monitoring takes the form of dynamic attack detection and recovery mechanisms. This implies a model of the attacker, which should at least cover all known types of attacks, for example in the form of an attack signature base. In this view, the safety-by-design principle becomes the security-by-design principle, meaning that the software must be designed from the foundation to be secure. This has led to design principles such as the OWASP recommendations. However, security and safety remain distinct and different domains, built on different hypotheses, and the protection mechanisms against accidental and intentional threats are usually complementary. In this white book we restrict our attention to security. [Cybercecurity: current challenges and Inria's research directions pp. 15-17]

III. Post-reading activities.

Task 7. Answer the following questions.

1. How does Wikipedia define cybersecurity?

Attack – спроба отримати несанкціонований доступ до послуг, ресурсів чи інформації Інформаційної системи або спроба порушити цілісність системи.

Attack surface – набір точок входу, де зловмисник може спробувати несанкціонований доступ. Заходи безпеки намагаються зберегти поверхню атаки якомога меншою.

Attackability – чутливість до зовнішніх подразників;

Authentication – перевірка заявленого значення атрибута.

Authentication – процес перевірки особистості фізичної або юридичної особи.

Authorization – а) вирішення питання щодо надання запиту на доступ (до суб'єкта) або б) призначенняправа доступу до комітента.

Balance of probabilities – наявність більшої вірогідності

Beyond a reasonable doubt - в повній мірі без сумнівів

Botnet – мережа скомпрометованих комп'ютерів (або ботів), яка контролюється зловмисником для запуску скоординованих шкідливих дій.

Breach – порушення

Bulletproof hosting service providers – постачальники, які, як відомо, не виконують вимоги щодо видалення правоохоронних органів. Це стає можливим завдяки розміщенню в країнах, де діє неміцне законодавство про кіберзлочинність, або операторам, що надають послуги, активно піддаючи місцевим правоохоронцям.

Byzantine – Аномальна поведінка, коли сутність / зловмисник надсилає різну (хоча і дійсну) інформацію різним одержувачам.

Calculi – числення;

card skimming – практика встановлення пристроїв в банкоматі, які дозволяють клонувати вкладені картки.

Carving – (вирізання вмісту файлу / даних) Процес відновлення та реконструкції вмісту файлу безпосередньо з блокової пам'яті без використання метаданих файлової системи. Взагалі, різьблення даних (структури) – це процес реконструкції логічних об'єктів (таких як файли та записи бази даних) із масового збору даних (образ диска / оперативної

Short glossary of cybersecurity terms

Access control – контроль за доступом;

Accommodate – адаптуватися, пристосуватися;

Accountability – підзвітність;

Ad hoc – який створюється в окремому випадку

Addressing scheme – метод адресації;

Adequacy decision – рішення про достатність заходів

Adjust – відрегулювати;

Admissible evidence – допустимі докази

Advocate – захищати, підтримувати;

Affirmative defence – заява про факти, що спростовують позов або звинувачення

Affirmative defences – заява про факти, що спростовують позов або звинувачення

Aforementioned – вищезазначений;

Anticipate – передбачити;

Anti-trust law – антимонопольний закон

Appification – Заміна веб-сайтів програмами, що працюють на мобільних пристроях.

Application – програма, додаток;

Arrest warrant – ордер на право арешту

Ascertain – переконати;

ASIC – це один клас інтегральних мікросхем, де схема налаштована на конкретну програму або набір програм. Наприклад TPM - цевиділений ASIC для програм безпеки.

Asset seizure – конфіскація майна

Assumption of risk – взяти на себе провину

Assumption – допущення, гіпотеза;

2. What does security include?
3. What physical security may depend on?
4. For what cybersecurity requires some form of physical security?
5. Do attackers follow predefined rules or continuously search for previously unknown means of attack?
6. Does digital information may play with contradictions between the legislations of different countries or their maladaptation to the digital age?
7. What software safety calls for?
8. Do safety and security tied to one another?
9. What does Ensuring safety mean?
10. What form takes the monitoring?

Task 8. Complete the following sentences using the text.

1. Wikipedia defines cybersecurity as follows: Computer security, also known as _____ _____ or IT security, is the protection of computer systems from the damage to their _____, software or information, as well as from disruption or misdirection of the services they provide.
2. Conversely, physical security may _____ _____ cybersecurity to the extent that it uses computer systems, e.g., to monitor some physical space or maintain a database of authorized persons.
3. Hence, an attack or malware launched by a _____ _____ can spread worldwide, at a large-scale, in less than an hour.
4. Digital information _____ _____, and may even play with contradictions between the legislations of different countries or their maladaptation to the digital age.
5. A complementary approach consists in describing normal execution paths and monitoring execution, so as to raise an alarm and react appropriately when some trajectory goes outside of _____ _____.

6. Since security works in an _____ _____, it should also consider accidental threats which may be exploited by the attacker.

7. Dealing with the safety of large _____ _____ that interact with the physical world, such as Cyber-Physical Systems (often known as CPS), has led to some well established methodologies.

8. Formally, one writes a _____ _____ to describe the expected behavior of the software, and then shows that the actual implementation satisfies the specification.

9. Monitoring takes the form of dynamic _____ _____ and recovery mechanisms.

10. However, security and _____ remain distinct and different _____, built on different hypotheses, and the protection mechanisms against accidental and intentional threats are usually complementary.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Кібербезпека – одна з основних проблем сьогодення

Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Сьогодні ми все більше й більше використовуємо їх у своїй діяльності. Не є винятком і Збройні Сили. Але взявши на службу телекомунікації і глобальні комп'ютерні мережі, слід знати й розуміти, які можливості для зловживання створюють ці технології. Сьогодні жертвами хакерів можуть стати не лише люди, але й цілі держави. За ефективністю та наслідками застосування кіберзброю, а саме такий термін

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Що таке крадіжка особистих даних?

Злодії, які займаються викраденням даних, зазвичай, отримують особисту інформацію, таку як паролі, номери ID, кредитних карток або номери соціального страхування, та використовують ці дані від імені жертви. Викрадена конфіденційна інформація може бути використана для різних незаконних цілей, зокрема для отримання кредитів, здійснення онлайн-покупок або для отримання доступу до медичних та фінансових відомостей жертви.

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Крадіжка особистих даних, особиста інформація, паролі, кредитні картки, соціальне страхування, жертва, незаконні цілі, конфіденційна інформація, онлайн-покупка.

people and safeguard against any mishappenning on the internet. Further, stronger laws have been formulated with respect to protection of “sensitive personal data” in the hands of the intermediaries and service providers (body corporate) thereby ensuring data protection and privacy.

III. Post-reading activities.

Task 7. Answer the following questions.

1.Is the time theft a crime?

2.How can we prevent time theft?

3. What do you know about intellectual property theft?

4 What does an identify theft involve?

Task 8. Complete the following sentences using the text.

1 An identity theft involves both _____therefore the provisions with regard to forgery as provided under the Indian Penal Code.

2 Some of the Sections of IPC such as _____ (Section 464), making false documents (Section 465), forgery for purpose of cheating (Section 468), reputation (Section 469

3 Cyber theft is a part of _____which means theft carried out by means of computers or theInternet.

4 The most common types of cyber theft _____identity theft, password theft, theft of information, internet time theftsetc.

5 Time card theft is a crime, thoughit is not usually _____unless the theft is substantial.

6 Intellectual property (IP) _____ is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc.

7 One of the most commonly and dangerously known _____of IP theft is counterfeit goods and piracy.

все частіше використовують вчені, можна прирівняти до зброї масового ураження. Тому кібербезпека – одна з основних проблем, що викликає занепокоєння. І чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем. Оскільки критичні вразливості в програмному забезпеченні та автоматизованих системах викликають небезпідставні побоювання, то не дивно, що уряди та суспільство в усьому світі шукають кращих заходів і методів для захисту особистих даних Інтернет-ресурсів від кіберзагроз.

На підтвердження попередніх слів, під час проведення зустрічі на вищому рівні глав держав та голів урядів країн – учасниць Північноатлантичного альянсу, яка проходила у 2016 році у Варшаві, було підписано перший в історії договір між ЄС та НАТО про співпрацю у сфері безпеки, зокрема в питаннях гібридних війн та кібератак. Кіберпростір, поряд із землею, повітрям, морем і космосом, визнано новим оперативним простором, а кібероперації – невід’ємною частиною гібридної війни. Найбільше уваги операціям у кіберпросторі приділяють такі провідні країни світу як Сполучені Штати Америки, Великобританія, Китай та ін. У них у бюджеті закладено величезні кошти на розвиток кібернетичної складової збройних сил, а також постійно втілюються в життя програми для забезпечення національної безпеки та захисту об’єктів критичної інфраструктури від кібератак. Оскільки ніхто не може з упевненістю стверджувати, що його мережі повністю захищені та можуть протистояти багатовекторним кібератакам, кібернетична безпека стала пріоритетом розвитку сучасної армії.

Заходи щодо реалізації Концепції кібербезпеки.

Для мінімізації ризиків у Європі в 2018 році наберуть чинності закони про захист даних. Вони передбачають різке підвищення штрафів за розголошення або втрату персональних даних, що змусить компанії вже в цьому році переглянути свої підходи і стандарти щодо забезпечення інформаційної та кібернетичної безпеки, в тому числі ввести окрему посаду

відповідального за захист інформації та кібернетичну безпеку. Важливим фактором посилення заходів кібернетичної безпеки є збереження балансу між комфортом, свободою доступу до інформації та забезпеченням надійного захисту інформації, від яких багато в чому залежить благополуччя громадян і мир в Україні. Однак це завдання непросте, і його доведеться вирішувати ще довгий час. Масштабна кібератака на корпоративні та державні мережі за допомогою вірусу «NotPetya», яка відбулася 27 червня 2017 року, – яскравий приклад важливості кібернетичної безпеки для функціонування держави. Подібні кібератаки спрямовані на дестабілізацію України. «Відключити, знищити, дестабілізувати», – ось їхня мета. Масові відключення електроенергії, телефонного зв'язку та Інтернету, труднощі з обслуговуванням клієнтів і проведенням банківських операцій, реальні фінансові збитки – це те, що використовує ворог вже сьогодні.

Використовуючи кіберпростір, хакери можуть зламати захищені мережі та отримати необхідну інформацію, тому ми мусимо спрямувати зусилля на захист своїх мереж і забезпечити їх безпеку, використовуючи такі рівні захисту інформації:

- запобігання – доступ до інформації та технології надається тільки для персоналу, який отримав допуск та має відповідні фахові навички;
- виявлення – забезпечується раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені;
- обмеження – зменшується розмір втрат, якщо злочин все-таки відбувся, незважаючи на заходи щодо його запобігання та виявлення;
- відновлення – забезпечується ефективне відновлення інформації за наявності документованих і перевірених планів з відновлення.
- Висновок, який ми повинні зробити для себе, – це збільшення інвестування в кібербезпеку, щоб запобігати атакам на великі державні й приватні компанії і протистояти намірам дестабілізувати суспільство.

Крім того, кожне суспільство потребує правил, стандартів, норм, положень, інструкцій та інших документів, щоб почувати себе захищеним у

An identity theft involves both theft and fraud, therefore the provisions with regard to forgery as provided under the Indian Penal Code, 1860 (IPC) is often invoked along with the Information Technology Act, 2000. Some of the Sections of IPC such as forgery (Section 464), making false documents (Section 465), forgery for purpose of cheating (Section 468), reputation (Section 469), using as genuine a forged document (Section 471) and possession of a document known to be forged and intending to use it as genuine (Section 474) can be coupled with those in the IT Act.

The Information Technology Act, 2000 (IT Act) is the main act which deals with the legislation in India governing cybercrimes. Some of the Sections dealing with Cyber Theft are: -

- Section 43 If any person without permission of the owner damages to computer, computer system, etc. he/she shall be liable to pay compensation to the person so affected.
- Section 66 If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
- Section 66B Punishment for dishonestly receiving stolen computer resource or communication device is Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
- Section 66C provides for punishment for Identity theft as: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.
- Section 66 D on the other hand was inserted to punish cheating by impersonation using computer resources.

With the increase in the number of frauds and cyber related crime, the government is coming up with refined regulations to protect the interest of the

Secondly, what is theft in cyber crime? Cyber theft is a part of cybercrime whichmeans theft carried out by means of computers or theInternet. The most common types of cyber theftinclude identity theft, password theft, theftof information, internet time theftsetc.

Furthermore, is time theft a crime?

Time card theft is a crime, thoughit is not usually prosecuted unless the theft issubstantial.

How can we prevent time theft?

Ways to Prevent Time Theft

- Choose the Right Time Tracking Method. There are many ways oftracking time and attendance, the most popular options being thefollowing:
- Improve Communication. It may seem obvious, but telling youremployees all your rules and expectations will prevent timetheft.
- Audit Your Processes.

Internet time theft

It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.

Theft of intellectual property

Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. One of the most commonly and dangerously known consequence of IP theft is counterfeit goods and piracy.

Laws governing identity thefts in India

The crime of identity theft consists of two steps:

- Wrongful collection of personal identity of an individual
- Wrongful use of such information with an intention of causing legal harm to that person information

кіберпросторі хоча б у правовому відношенні. Зараз з'являються галузеві нормативні документи, що стосуються кіберризиків, зростає інтерес до цієї галузі з боку законодавчих органів.

Task 11. Give the English equivalents of the Ukrainian words and word combinations.

Хакери, інформаційне суспільство, інтернет-ресурси, кіберпростір, програмне забезпечення, автоматизовані системи, кіберзагрози, розвиток кібернетичної складової збройних сил, масові відключення електроенергії, ЄС, НАТО, гібридна війна, кібератаки, кібероперації, кібернетична безпеки, кіберризик, корпоративні та державні мережі, зламати захищені мережі, захист інформації, механізм захисту, доступ до інформації, ефективне відновлення інформації, раннє виявлення злочинів і зловживань, зменшити розмір втрат, збільшення інвестування в кібербезпеку.

Unit 2. A few examples and lessons learned

I. Pre-reading activities.

Task 1. How do you understand the statement: *"If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you".* (Stephane Nappo) **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What definitions of the ransomware do you know?
2. What do you understand under the term cybersecurity incidents?
3. What is the most common synonym to the word attack?

Task 3. Try to guess the meaning of the following words.

Vulnerable systems, a viral manner, default accounts, deleting firmware, unconfigured services, remotely controlled bots, exploitation, anonymized databases.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

This ransomware targets computers running the Microsoft Windows operating system, with major consequences for their owners: are infecting a computer, the ransomware encrypts data and displays a note to inform the user, asking for 1). a bitcoin payment in exchange for 2). the decryption key. This ransomware is considered a worm, since it scans for vulnerable systems and then 3). replicates itself on these new targets. 4). Electronic voting vulnerabilities: in the last few years, several European countries (Estonia, France, Norway, and

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. illegal means	a) кіберкрадіжка
2.attendance	b) варіант
3. access to	c) пароль
4. password	d) доступ до
5. option	e) відвідуваність
6. cyber theft	f) незаконні засоби

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What is considered to be the time theft?
2. When does the time theft occur?
3. What is the theft in cyber crime?

Internet time thefts

Internet time theft. It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The authorized personget access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.

Then, what is considered time theft?

Time theft at work occurs when an employeeaccepts pay from their employer for work that they have notactually done, or for time they have not actually put intotheir work. Since the employee is not actually doing the necessary amount of work during their shift it is considered atheft of time from the company.

Unit 22. Internet time thefts

I. Pre-reading activities.

Task 1. How do you understand the statement: *One of the most commonly and dangerously known consequence of IP theft is counterfeit goods and piracy*. **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What do you know about cyber theft?
2. What do you understand under the term hacking ?
3. What is theft in cyber crime?

Task 3. Try to guess the meaning of the following words

Cyber crime, cyber theft, password theft, intellectual property.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. The authorized persongets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.
2. Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet.
3. There are many ways of tracking time and attendance, the most popular options being thefollowing:
4. It may seem obvious, but telling your employees all your rules and expectations will prevent time theft.

Switzerland) held legally binding 5). political elections that allowed part of the voters 6). to cast their votes remotely 7). via the Internet.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1). cybersecurity	a). виконувати
2). internal	b). невідповідність
3). a victim	c). поданий голос
4). a password	d). кібербезпека
5). a cast vote	e). виконувати
6). to perform	f). пароль
7). an inadequacy	d). жертва

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. Can you provide a few illustrative examples of attacks highlighted in the text?
2. Who found that The TV5 Monde target attack was carefully planned?
3. What allows attackers to create a strobe effect?

A few examples and lessons learned

Unfortunately, cybersecurity incidents are common, and too often make the headlines. Here we describe a few illustrative examples, in order to highlight the huge diversity of attacks. Some of them target well identified entities, such as TV5 Monde and the Dyn company, although the attacks used totally different techniques. At the other end of the spectrum the Wannacry ransomware targeted a

huge population, propagating in a viral manner. Certain electronic voting systems are known to be vulnerable and, on several occasions, security researchers have highlighted their inadequacy through proof-of-concept attacks. The following example illustrates how anonymized databases can sometimes be attacked, revealing physical identities. The last two examples highlight, for the first one, two hardware-targeted software attacks that exploit advanced processor performance optimization techniques, and for the second one, weaknesses of some Internet of Things devices and their exploitation.

The TV5 Monde targeted attack: on April 9th, 2015 the French TV network TV5 Monde was the victim of a major sabotage. Around 9pm, the website and social media channels (Facebook, Twitter, YouTube) were defaced. About an hour later, the network infrastructure was no longer operational and broadcasting was interrupted, resulting in a complete TV blackout – the worst thing that can happen to a TV network. The French National Cybersecurity Agency (ANSSI) later found that the attack was carefully planned. The attackers first connected in January, using a stolen login and password. This allowed them to get access to the internal network, to collect internal documents containing information on the network infrastructure and existing accounts, and to exploit unconfigured services that still relied on default accounts and passwords. Deleting firmware on the network infrastructure (routers and switches) then caused the breakdown, making a simple restart impossible. Denial of service attacks from the Mirai botnet of home devices: the Mirai malware's goal is to turn vulnerable home devices (such as IP cameras, printers, baby monitors, or home routers) into remotely controlled bots that can later be used to launch large-scale denial of service attacks. This is what happened on October 21st, 2016, when this botnet targeted the name servers of the Dyn company. This attack resulted in a blockage of many web sites worldwide for several hours. The WannaCry ransomware: on Friday May 12th, 2017, the WannaCry ransomware propagated throughout the world, infecting more than 230,000 computers in over 150 countries within a single day (source Wikipedia). This ransomware targets computers running the Microsoft Windows operating

4. The request for authentic information from the victim (e.g., a user account) causes the _____to sign the user out.
5. The attacker uses the user's user _____to log in as the victim.
6. The user is then shown _____login form that uses the user name and password for the malicious site.
7. If the user is tricked into _____the fake login form, the host site or the cloud storage site is logged out of the account.
8. This means that the user's legitimate account is _____of his or her account as well.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Web Jacking Attack Vector – ще одна фішинг-техніка, яка може бути використана в соціальних інженерних заходах. Зловмисники, які використовують цей метод, створюють підроблений веб-сайт, і коли жертва відкриває посилання, з'являється сторінка із повідомленням про те, що веб-сайт перемістився і їм потрібно щоб натиснути інше посилання. Якщо жертва натискає посилання, яке виглядає реальним, він буде перенаправлений на фальшиву сторінку.

Набір інструментів соціальної інженерії вже імпортував такий вид атак, тому ми збираємося використовувати SET для реалізації цього методу. Ми відкриваємо SET і вибираємо варіант 2, який є Вектор атаки веб-сайтів.

Джерело: https://www.jigsawacademy.com/blogs/cyber-security/web-jacking

the link and type your computer's IP address here. It will create a link. Now, your link is ready to copy and send to the victim, then wait until they enter their details.

Step 7: When the victim opens a link in their browser, the browser displays the message "help www.abc.com move to another address, click here to go to a new location," and click this link, they will find it redirected to a fake webpage.

3. HOW TO BE SAFE FROM THE WEB JACKING ATTACK METHOD?

Users who receive emails with phishing links should always check the URL first by typing the URL in the address bar rather than clicking the link. If the URL does not match the expected website, the user should not click on the link and should also not click on any suspicious links in emails. Users should also avoid clicking on links sent in emails with an embedded image or if the sender starts with a link that looks like a typical URL.

III. Post-reading activities.

Task 7. Answer the following questions.

1. How to be safe from the Web Jacking attack method
2. What does the browser display when the victim opens a link
3. What must users avoid when open a link
4.

Task 8. Complete the following sentences using the text.

1 A hacker _____a free domain name that is the same as the domain of a web application.

2 Using a ____attack vector, the attacker sets up the real site to be malicious and lies about the domain name of the real site.

3. The attacker sends a request to the_____ web application using the domain of the malicious site.

system, with major consequences for their owners: are infecting a computer, the ransomware encrypts data and displays a note to inform the user, asking for a bitcoin payment in exchange for the decryption key.

This ransomware is considered a worm, since it scans for vulnerable systems and then replicates itself on these new targets. Electronic voting vulnerabilities: in the last few years, several European countries (Estonia, France, Norway, and Switzerland) held legally binding political elections that allowed part of the voters to cast their votes remotely via the Internet. French people living abroad were allowed to vote via the Internet for the June 2012 parliamentary elections. An engineer demonstrated that it was possible to write malware that could change the value of a cast vote, with no way for the voter to know.

In the 2011 Estonian parliamentary election, a similar attack was reported by computer scientist Pihelgas, who conducted a real-life experiment with fully aware subjects. Re-identification in the AOL anonymized database of web search queries: as reported in the New York Times 5, AOL released an anonymized database containing more than 20 million web search queries. Even though the data was anonymized, users could be identified are some investigation, thereby revealing all their personal search queries. More generally, database anonymization is a complex task with pitfalls, that requires finding an appropriate balance between utility and privacy. The Spectre and Meltdown vulnerabilities: on January 3rd, 2018, two hardware vulnerabilities, Spectre and Meltdown, were simultaneously released. Both vulnerabilities exploit speculative execution (and in particular branch prediction), an optimization technique in modern processors. To avoid idle processor cycles, e.g., while waiting for the result of a memory access, processors may perform out-of-order execution. A branch may then be speculatively executed, while waiting for the evaluation of a conditional. If the branch was wrongly executed, the results are discarded. However, even if the results are discarded, a memory access nevertheless leaves a trace in the cache. The idea of the Spectre and Meltdown attacks is to force a forbidden memory access. Typically, buffer overflows are prevented by checks on the size of the buffer. These checks can be

circumvented however by making the branch prediction wrongly predict the test. Then, a cache attack can be used to check which area of the memory has been executed. (Such attacks simply measure the time necessary for accessing a particular memory address.)

The attacks are particularly severe, because they exploit the design of modern processors, and cannot be simply patched by a software update. Moreover, speculative execution is at the core of modern processor design, and is unlikely to be abandoned by processor manufacturers. Smart lights causing epilepsy seizures: researchers from the Weizmann Institute of Science have shown that it is possible to hack commonly deployed smart lights, and to strobe them at a frequency that may trigger epileptic seizures. The attack is interesting because by turning traditionally unconnected objects (here, light bulbs) into smart objects, they can be misused to create an unexpected attack. This particular attack exploits a combination of several flaws. First, when initializing the smart light controller, the password that allows the controller to connect to the local WiFi is sent unencrypted and can easily be sniffed. Second, the lights accept commands from any devices on the local WiFi without a proper authentication mechanism. Third, the controller does not verify the length of the commands it receives, allowing the concatenation of multiple commands, circumventing the limit on commands that may be sent per second. Finally, the attack is based on undocumented API options, allowing attackers to create a strobe effect. [Cybercecurity: current challenges and Inria's research directions pp. 18-21]

III. Post-reading activities.

Task 7. Answer the following questions.

1. What does the lights accept from any devices on the local WiFi without a proper authentication mechanism?
2. How a cache attack can be used?
3. What is considered a worm?

5. The attackers often use malicious scripts that work with popular cloud storage sites such as DropBox or Google Drive. After the malicious script is uploaded to the hosting service or cloud storage site, the malicious user name and/or password are displayed on the account page.

6. The user is directed to a login page hosted on the hosting service or cloud storage site. The user is then asked to enter his or her own user name and/or password. The user is then shown a fake login form that uses the user name and password for the malicious site. If the user is tricked into entering the fake login form, the host site or the cloud storage site is logged out of the account. This means that the user's legitimate account is logged out of his or her account as well.

7. The attacker is now able to log into the victim's account. This is because the victim's account was logged out when the user visited the login page. The attacker can now use the victim's legitimate account to download any file the victim has on the host server or cloud storage site. The attacker can also delete any files stored on the cloud storage site, and users are never alerted to the incident.

2. HOW TO APPLY WEB JACKING ATTACK METHOD

Step 1: To use the web jacking attack method, we will use a tool in kali Linux called setoolkit.

Step 2: Open your kali Linux system, then open the Terminal window.

Step 3: Type a deadly setoolkit.

Step 4: It will show many ways to attack, but you will have to choose a Social-engineering attack.

Step 5: Type 1 to choose a Social-engineering attack. It will show multiple methods of engineering attack. Here, you have to select a vector to attack the website, so type 2 will show different ways to attack it.

The above methods will create a fake webpage similar to the victim's web page and host it on your computer.

Step 6: Copy the link (IP of your computer that you previously installed) to the fake website and send it to the victim. If the link is your home IP address, then change it to a domain name. To convert your IP address to a domain name, open

often used to gain corporate or government networks as part of a larger attack, such as an Advanced Persistent Threat (APT). In the latter case, employees are compromised to go through security perimeters, distribute malware within a closed area, or gain access to secure data. An organization defeated by these attacks often supports greater financial losses in addition to declining market share, reputation, and consumer confidence. Broadly speaking, a criminal attempt to steal sensitive information can escalate into a security incident where the business will have a difficult time recovering.

1. WEB JACKING ATTACK METHOD

The setup for the attack is simple:

1. A hacker registers a free domain name that is the same as the domain of a web application. Using a generic attack vector, the attacker sets up the real site to be malicious and lies about the domain name of the real site.

2. The attacker sends a request to the legitimate web application using the domain of the malicious site. The request for authentic information from the victim (e.g., a user account) causes the web application to sign the user out. The attacker uses the user's user name and password to log in as the victim.

3. The attacker can now use the victim's user name and password to log in as the victim. If the attacker uses the name and password for the victim's account, they can access any information from the victim's account on the legitimate website. The attacker can now send an authentication request with the victim's real name and password to its legitimate website. The victim's account will only accept this request if the user name and password match the attackers.

4. The attacker signs up for a free domain name that contains one or more numbers or special characters. Using the official domain name of the site as the source of the registration, the attacker registers an account at a hosting service or cloud storage site. Using this account, the attacker posts a malicious script to the host site that contains the malicious user name and/or password. The script performs a malicious action on behalf of the victim.

4. How anonymized databases can sometimes be attacked?
5. What is a complex task with pitfalls, that requires finding an appropriate balance between utility and privacy?
6. Who demonstrated that it was possible to write malware that could change the value of a cast vote, with no way for the voter to know?
7. What is the idea of the Spectre and Meltdown attacks?
8. Which European countries held legally binding political elections that allowed part of the voters to cast their votes remotely via the Internet?
9. When may processors perform out-of-order execution?
10. How long was the network infrastructure no longer operational and was broadcasting interrupted?

Task 8. Complete the following sentences using the text.

1.The _____ are particularly severe, because they exploit the design of modern processors, and cannot be simply patched by a software update.

2. More generally, _____ _____ is a complex task with pitfalls, that requires finding an appropriate balance between utility and privacy.

3. The idea of the Spectre and Meltdown attacks is to force a forbidden _____ _____.

4. _____, the attack is based on undocumented API options, allowing attackers to create a strobe effect.

5. Deleting firmware on the _____ infrastructure (routers and switches) then caused the breakdown, making a simple _____ impossible.

6. _____ _____ _____ speculative execution (and in particular branch prediction), an optimization technique in modern processors.

7. Unfortunately, _____ incidents are common, and too often make the headlines.

8. A _____ may then be speculatively executed, while waiting for the evaluation of a _____.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Кіберзлочинність під час пандемії. Що нового дізналися спецслужби Німеччини?

Під час пандемії в Німеччині зросла кількість злочинів, скоєних в інтернеті. На кого націлені хакерські атаки, і що нового дізналися фахівці BKA, котрі підготували щорічний звіт. 108 474 кіберзлочини було зареєстровано в 2020 році в Німеччині. Такі дані містяться в щорічній доповіді німецького Федерального управління кримінальної поліції (BKA). Це майже на 8 відсотків більше, ніж у 2019 році. При цьому число незареєстрованих злочинів у мережі може бути набагато «вище середнього», вважає експерт цього відомства Карстен Майвірт (Carsten Meywirth). З квітня 2020 року він очолює в BKA спеціальний відділ, який займається розслідуванням кіберзлочинів, число яких стрімко зростає.

Німеччина як один з економічних та інноваційних центрів є привабливою метою для хакерів з усього світу. Має значення і її геостратегічне розташування – в самому серці Європи. «Вплив у ЄС і членство в НАТО роблять Німеччину однією з основних цілей для кіберзлочинців», - каже Карстен Майвірт.

Він зазначає, що під час пандемії у хакерів з'явилися нові цілі: портали, пов'язані з виробництвом і розподілом вакцини, навчальні платформи, сервери, що дозволяють працювати в режимі хоум-офісу. Особливо цікавить кіберзлочинців весь ланцюг постачання й розподілу вакцин проти коронавірусу, оскільки "якщо вийде з ладу хоча б одне підприємство, задіяне в цьому, це буде мати величезні наслідки для суспільства", каже Майвірт.

1. criminal attempt	a) зловмисне посилання
2. freezing	b) замах на злочин
3. malware	c) заморожування
4. recipient	d) шкідливе програмне забезпечення
5. ransomware	e) одержувач
6.malicious link	f) програма-вимагач

II. <u>While-reading activities.</u>

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What is Phising attack used for?
2. Which consequences does the attack have?
3. How to apply Web Jacking method?

Web jacking

When a Web application improperly redirects a user's browser from a page on a trusted domain to a bogus domain without the user's consent, it's called Web Jacking. Web Jacking attack method is another type of social engineering attack method called Phishing attack, often used to steal user data, including login credentials and credit card numbers. When an attacker impersonating an object, cheats the victim by opening an email, instant message, or text message. The recipient is then tricked into clicking on a malicious link, leading to a malware installation, program freezing as part of a ransomware attack, or exposure to sensitive information.

Attacks can have serious consequences. For individuals, this includes unauthorized purchases, money laundering, or identity theft. Also, identity theft is

Unit 21. Web jacking

I. Pre-reading activities.

Task 1. How do you understand the statement: *Attacks can have serious consequences. "***Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What do you know about Web Jacking?
2. What is the setup to the attack?

Task 3. Try to guess the meaning of the following words.

Engineering attack, bogus domain, login credentials, instant message ,impersonating, program freezing.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. Web Jacking attack method is another type of social engineering attack method called Phishing attack
2. When an attacker impersonating an object, cheats the victim by opening an email, instant message, or text message.
3. The recipient is then tricked into clicking on a malicious link, leading to a malware installation, program freezing as part of a ransomware attack, or exposure to sensitive information.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

https://www.dw.com/uk/kiberzlochynnist-pid-chas-pandemii-shcho-novoho-diznalysia-spetssluzhby-frn/a-57499545

Що робити, якщо ваші персональні дані продають в інтернеті?

Останній «злив» даних українців, які продаються у Telegram-каналах, привернув увагу до проблеми незахищеності персональної інформації в Україні. Чи захищені ваші персональні дані і що робити, якщо ними вже торгують?

Останній кіберскандал, коли злочинці отримали доступ до персональних даних 26 мільйонів українців і торгували ними завдяки анонімних ботів у месенджері Telegram, оголив «дірки» в українській системі захисту персональної інформації. Хоча подібні «витоки» були й раніше, однак зараз звинувачення лунають на адресу державного застосунку «Дія», який останнім часом активно популяризує міністерство цифрових трансформацій України. На анонімних Telegram-каналах дехто з українських громадян знайшов інформацію про свої "свіжі" водійські посвідчення, які реєструвалися в «Дії».

Шпарина в «Дії»?

Голова громадської організації «Електронна демократія» Володимир Фльонц одним з перших забив на сполох. Перевіряючи свої дані через анонімного бота в Telegram, виявив там інформацію про свій внутрішній і закордонний паспорти, водійське посвідчення і навіть паролі від своєї електронної пошти. «Бази даних українців давно гуляють в інтернеті. Але вперше у відкритому доступі з'явилися свіжі фото з документів, які вважалися захищеними. Здивувало, як ця інформація була об'єднана з різних джерел. Якщо раніше бази були доступні окремо, то зараз бот надавав всю інформацію об'єднано, і банківську, і фото, номери телефонів, і паролі з соцмереж по людині», – розповів DW Володимир Фльонц. Він не виключає, що масовий «витік» стався безпосередньо з державних реєстрів, а мобільним додатком «Дія», який є верхівкою інфраструктури цих реєстрів, зловмисники скористалися як шпариною. Всі звинувачення на адресу державного

застосунку «Дія» міністр цифрової трансформації Михайло Федоров відкидає. «Це неможливо навіть теоретично! По-перше і головне, «Дія» не має бази даних і не накопичує таку інформацію. По-друге, кількість інформації, яка доступна у зазначеному боті, набагато, в десятки, а то й сотні разів, перебільшує ту, з якою працює «Дія», – написав Федоров на своїй сторінці у соціальній мережі Facebook.

Кіберполіція України оперативно заблокувала анонімний Telegram-бот, а головне слідче управління Нацполіції України відкрило кримінальне провадження за ознаками кримінального правопорушення, передбаченого 361 Кримінального кодексу України (несанкціоноване втручання в роботу електронно-обчислювальних машин, комп'ютерних мереж чи мереж електрозв'язку). Після проведення слідчих дій поліція не виявила фактів кібератак на державний мобільний застосунок «Дія».

«Інформація, поширена у соціальних мережах, зокрема і в Telegram-каналах, має ознаки фрагментарних наборів даних, скомпільованих з різних джерел і ресурсів, включаючи відкриту інформацію із реєстрів», - йдеться у повідомленні на сайті Нацполіції. https://www.dw.com/uk

Task 11. Give the English equivalents of the Ukrainian words and word combinations.

База даних, електронно-обчислювальна машина, зловмисники, мобільний застосунок «Дія», водійське посвідчення, мережа електрозв'язку, персональні дані, системі захисту, пандемія, кіберскандал, навчальні платформи, вакцини проти коронавірусу, Голова громадської організації, доступ до персональних даних, інноваційний центр, звинувачення, міністерство цифрових трансформацій України, масовий «витік» інформації, анонімний Telegram-канал, режим хоум-офісу, скомпільований з різних джерел, верхівка інфраструктури, Кримінальний кодекс України, хакери.

Зловмисники також можуть використовувати комбінацію шпигунських та логічних бомб, намагаючись вкрасти вашу особу. Наприклад, кіберзлочинці використовують шпигунські програми, щоб приховано встановити кейлоггер на комп’ютер. Keylogger може фіксувати ваші натискання клавіш, такі як імена користувачів та паролі. Логічна бомба призначена для того, щоб зачекати, поки ви відвідаєте веб-сайт, який вимагає увійти за допомогою своїх облікових даних, наприклад, на банківському сайті або в соціальній мережі. Отже, це спровокує логічну бомбу для виконання кейлоггера та захоплення ваших облікових даних та надсилання їх віддаленому зловмиснику. Джерело: https://www.avast.com/c-what-is-a-logic-bomb?v=rc

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Банківський сайт, логічна бомба, захоплення облікових даних, віддалений зловмисник, натискання клавіш, імена користувачів, довільний код, запуск програми.

Task 8. Complete the following sentences using the text.

1. Logic bombs are subtle, sophisticated cybersecurity attacks — but the _____can be explosive.
2. This article will define_____, explain how they work, and explore famous logic bomb attacks.
3. Logic bombs are small _____contained in other programs.
4. Although they might be ____they're not technically malware — it's a fine line.
5. Common types of malware include viruses and worms, which can contain logic bombs as part of their_____.
6. A logic bomb virus would then be a _____that has a logic bomb in its code.
7. Anything that can _____the servers of a large company or institution has the power to cause serious havoc to the organization itself and the general population it serves.
8. Considering the potential _____of such a threat, it's critical to protect yourself against logic bombs and other malware threats.

Task 9. Make a list of all the terms/procedures/experiments/pieces you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Логічна бомба – це зловмисне програмне забезпечення, яке викликається відповіддю на подію, наприклад, запуск програми або коли досягається конкретна дата / час. Зловмисники можуть використовувати логічні бомби різними способами. Вони можуть вбудовувати довільний код у підроблену програму або троянський кінь, і він буде виконуватися щоразу, коли ви запускаєте шахрайське програмне забезпечення.

Unit 3. Risk assessment and management methods

I. Pre-reading activities.

Task 1.How do you understand the statememnt: *"The biggest risk is not making any risky decisions… In a world that is changing very fast, the only strategy that is guaranteed to fail is not to take risks"* (Mark Zuckerberg, founder of Facebook).
Translate into Ukrainian.

Task 2. Discuss the following questions.

1.Can you name the methods of capturing the four elements of risk?
2.What do you understand uner the term risk?
3.What is the most synonym to the word oil?

Task 3. Try to guess the meaning of the following words.

Cyber risk, relevant actors, preventing, vulnerabilities, core areas, crosscutting components.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

There are a 1). range of methods, some of which have been established as international standards and guidelines, that provide a structured means to transform vulnerability, threat, likelihood and impact into a ranked list in order to be able to prioritise and treat them. 2). Pre-assessment includes 3). the framing of risk, identification of relevant actors and stakeholders, and captures perspectives on risk. A step-by-step detailed guide can be found in the 4). full document, but we summarise the actions here. It also involves 5). defining assumptions and

constraints on elements such as resources required and predisposing conditions that need to inform the risk assessment. The assessment approach and tolerances for risk are also defined at this stage along with 6). identifying sources of information relating to 7). threats, 8). vulnerabilities and impact.

Task 5. Match the English phrases on the left their Ukrainian equivalents on the right.

1). pre-assessment	a). ймовірність
2). ranked list	b). таксономія
3). likelihood	c). зацікавлені сторони
4). prerequisites	d). рейтинговий лист
5). a taxonomy	e). наскрізний
6). stakeholders	f). передумови
7). cross-cutting	g). попередня оцінка

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What is the purpose of capturing the four elements of risk?
2. What is the assessment and characterization of risk management?
3. At what stage are threats identified?

Risk assessment and management methods

The purpose of capturing these four elements of risk is for use in dialogue that aims to represent how best to determine the exposure of a system to cyber risk,

- It lies dormant for a specific amount of time. Like a ticking time bomb, logic bombs aren't meant to go off right away. That's why people attacking from within a targeted system often use logic bombs – so they can cover their tracks. Logic bombs are subtle and can go undetected for years.
- Its payload is unknown until it triggers. A payload is the component of malware that carries out the malicious activity – basically, what sort of damage the malware is coded to inflict. The payload can result in anything from the spread of spam emails through an infected system or the theft of valuable data.
- It's triggered by a certain condition. The detonator of the logic bomb is the condition that must be met. It's this feature that lets logic code bombs go undetected for long periods of time. The trigger could be the deletion of an employee from the company payroll, or the date of an important event. Logic bombs with triggers related to dates or specific times are also known as time bombs.

As malware continues to grow more sophisticated, it's essential to keep a strong line of defense. Detect logic bombs and other malware threats automatically with Avast Free Antivirus. It uses intelligent threat-detection and real-time protection to stop malware threats in their tracks.

III. Post-reading activities.

Task 7. Answer the following questions.

1. Where is the logic bomb inserted?
2. What damage can the logic bomb cause?
3. Which powerful software security tools do you know?
4. Why do you need to use security tools?
5. What does common types of malware include?

a specific condition occurs. When this condition is met, the logic bomb is triggered – devastating a system by corrupting data, deleting files, or clearing hard drives.

Is a logic bomb malware?

Logic bombs are small bits of code contained in other programs. Although they might be malicious, they're not technically malware – it's a fine line. Common types of malware include viruses and worms, which can contain logic bombs as part of their attack strategy. A logic bomb virus would then be a virus that has a logic bomb in its code.

Unlike viruses and worms, which can infect a system on their own, a logic bomb is often inserted by someone with inside knowledge of the system – such as when a disgruntled employee embeds a logic bomb in their company's network. And since they're activated by a specific condition, logic bombs can go undetected for long periods of time, until they're triggered by the coded condition.

How does a logic bomb work?

The conditions that trigger a logic bomb can be categorized as positive or negative. Logic bombs with positive triggers detonate after a condition is met, such as when you open a particular file. Negative triggers launch a logic bomb when a condition is not met, such as when the bomb isn't deactivated in time.

Either way, when the desired conditions are achieved, the program's system of logic will order the logic bomb to go off and inflict its damage.

Logic bomb attacks can be devastating. There are instances (read more below) of how logic bombs have wiped the servers of major financial institutions and other organizations. Anything that can disrupt the servers of a large company or institution has the power to cause serious havoc to the organization itself and the general population it serves.

Considering the potential consequences of such a threat, it's critical to protect yourself against logic bombs and other malware threats.

What are the characteristics of a logic bomb virus?

The defining characteristics of a logic bomb are:

and how to manage it. There are a range of methods, some of which have been established as international standards and guidelines, that provide a structured means to transform vulnerability, threat, likelihood and impact into a ranked list in order to be able to prioritise and treat them. While each method has its own particular approach to risk assessment and management, there are some features common to a number of the most widely used methods that are useful for framing risk assessment and management activities, which can be mapped back to Renn's seminal work on risk governance as discussed in earlier sections.

The International Risk Governance Council (IRGC) capture these in its risk governance framework (developed by an expert group chaired by Renn), which includes four core areas and crosscutting components. Pre-assessment includes the framing of risk, identification of relevant actors and stakeholders, and captures perspectives on risk. Appraisal includes the assessment of causes and consequences of risk (including risk concern), developing a knowledge base of risks and mitigation options (e.g., preventing, sharing etc). Characterisation involves a decision process, making a judgment about the significance and tolerance of the risks. Appraisal and Characterisation forms the basis of the implementation of Renn's three core components of risk assessment. Management processes include deciding on the risk management plan and how to implement it, including risk tolerance (accepting, avoiding, mitigating, sharing, transferring). Cutting across all four is communication, engagement and context setting through open and inclusive dialogue.

The US Government NIST guidelines capture the vulnerability, threats, likelihood and impact elements inside the prepare (pre-assessment), conduct (appraisal and characterize), communicate (cross-cutting), maintain (management) cycle. A step-by-step detailed guide can be found in the full document, but we summarise the actions here. Prepare involves identifying the purpose (e.g., establishing a baseline of risk or identifying vulnerabilities, threats, likelihood and impact) and scope (e.g., What parts of a system/organization are to be included in the risk assessment?; What decisions are the results informing?). It also involves

defining assumptions and constraints on elements such as resources required and predisposing conditions that need to inform the risk assessment. The assessment approach and tolerances for risk are also defined at this stage along with identifying sources of information relating to threats, vulnerabilities and impact. Conduct is the phase where threats, vulnerabilities, likelihood and impact are identified. There are a range of ways that this can be conducted, and this will vary depending on the nature of the system being risk assessed and the results of the prepare stage.

NIST has a very specific set of tasks to be performed. These may not be relevant to all systems, but there are some useful tasks that generalize across multiple system perspectives, including identifying: threat sources and adversary capability, intent and targets; threat events and relevance to the system in question; vulnerabilities and predisposing conditions; likelihood that the threats identified will exploit the vulnerabilities; and the impacts and affected assets. Note that the ordering of actions in the NIST approach puts threat identification before vulnerabilities, which presupposes that all threats can be identified and mapped to vulnerabilities. It is worth highlighting that risk assessment must also be effective in situations where threats are less obvious or yet to be mainstream (e.g., IoT Botnets) and, therefore, some organizations that are particularly ingrained in digital adoption may also wish to consider conducting a vulnerability assessment independently or prior to the identification of likely threats to avoid making assumptions on what or who the threats actors may be.

A list of commonly used component-driven cyber risk management frameworks includes a brief description, an overview of how they work, who should use it, and an indication of cost and prerequisites. While not wishing to reproduce the whole list here, we provide an overview for the purposes of comparison.

- ISO/IEC 27005:2018 is an international standard set of guidelines for information risk management. It does not prescribe a specific risk

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. computer network	a) програмний додаток
2. operating system	b) операційна система
3.software application	c) псування даних
4. corrupting data	d) комп*ютерна мережа
5. deleting files	e) очищення жорстких дисків
6. clearing hard drives	f) видалення файлів

II. <u>While-reading activities.</u>

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What do you know about logic bombs?
2. How does the logic bomb work?
3. Is a logic bomb a virus ?

Logic bombs

Logic bombs are subtle, sophisticated cybersecurity attacks – but the damage can be explosive. This article will define logic bombs, explain how they work, and explore famous logic bomb attacks. We'll also show you how to protect yourself against all kinds of malicious cyber attacks with powerful software security tools like Avast Free Antivirus.

What is a logic bomb?

A logic bomb is a malicious piece of code that's secretly inserted into a computer network, operating system, or software application. It lies dormant until

Unit 20. Logic bombs

I. Pre-reading activities.

Task 1. How do you understand the statement: *"Logic bombs are subtle, sophisticated cybersecurity attacks — but the damage can be explosive* **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What is a logic bomb?
2. What are the characteristics of a logic bomb virus?
3. Is a logic bomb malware?

Task 3. Try to guess the meaning of the following words.

Cyber attacks , software application, malware triggers **,**disgruntled employee

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. Logic bombs are small bits of code contained in other programs.
2. It lies dormant for a specific amount of time.
3. And since they're activated by a specific condition, logic bombs can go undetected for long periods of time, until they're triggered by the coded condition.
4. Logic bomb attacks can be devastating.
5. There are instances of how logic bombs have wiped the servers of major financial institutions and other organizations.
6. The detonator of the logic bomb is the condition that must be met.

assessment technique but does have a component-driven focus and requires vulnerabilities, threats and impact to be specified.

- NIST SP800-30/39 are the US Government's preferred risk assessment/management methods and are mandated for US government agencies. They have a strong regulatory focus, which may not be relevant for countries other than the US, but they have a clear set of guiding steps to support the whole risk assessment and management process from establishing context to risk tolerance, and effective controls, including determining likelihood of impact. They are freely available and consistent with ISO standards (which are not free but are low cost).
- The Information Security Forum (ISF) produced the IRAM 2 risk management methodology that uses a number of phases to identify, evaluate and treat risks using the vulnerability, threats and impact measures. It is provided to (paid up) members of the ISF and requires information risk management expertise to use it effectively, which may come at additional cost.
- FAIR, initially developed by Jones and subsequently collaboratively developed with the Open Group into OpenFAIR, proposes a taxonomy of risk factors and a framework for combining them. Threat surface can be considered very broad and there is a clear focus on loss event frequency, threat capability, control strength and loss magnitude. It also breaks financial loss factors into multiple levels and supports a scenario model to build comparable loss profiles.
- Octave Allegro is oriented towards operational risk and security practices rather than technology. Qualitative risk assessment is linked with organizational goals. Real-world scenarios are used to identify risks through threat and impact analysis. The risks are then prioritized and mitigation is planned. The approach is designed for workshop style risk assessment and could be performed in-house possibly resulting in a lower cost than a consultant-led risk assessment.

- STRIDE is a failure-oriented threat modelling approach focusing on six core areas: spoofing (faking identity), tampering (unauthorized modification), repudiation (denying actions), denial of service (slowing down or disabling a system), and elevation of privilege (having unauthorized control of the system). The approach considers threat targets (including what an attacker may do), mitigation strategy, and mitigation technique. Threats can be considered for multiple interactions on the same threat target in the system and can include people, process and technology. Shostack presents STRIDE as part of a four-stage framework in his book – model the system, find threats, address threats, validate. Threat modelling, of course, cannot guarantee that all failures can be predicted, but the iterative process supports continual assessment of evolving threats if time and resources allow.
- Attack Trees formulate an overall goal based on the objectives of an attacker (the root node), and develop sub-nodes relating to actions that would lead to the successful compromise of components within a system. Like STRIDE, attack trees are required to be iterative, continually considering pruning the tree and checking for completeness. Attack libraries such as Common Vulnerabilities and Exposuress (CVEs) and Open Web Application Security Project (OWASP) can be used to augment internal knowledge of evolving threats and attacks.

III. Post-reading activities.

Task 7. Answer the following questions.

1. What does the preliminary assessment include?
2. What do management processes involve?
3. What decisions are the result of information?
4. What should be the risk assessment?
5. What does the list of common components include?

зловмисник, програміст, інформатика, соціальна мережа, особистий профіль, обмеження, захист, безпека, тестування, розслідування, жорсткий диск, макровірус, віруси-хробаки.

Коротка історія

Перша кампанія поширення небажаних електронних повідомлень через електронну пошту була зафіксована 1978 році під час якої розсилку отримали майже 400 (або 15% всіх) користувачів, підключених до попередника мережі Інтернет – ARPANET. Кампанія рекламувала презентацію продукту компанії, але після отримання великої кількості негативних відгуків ця форма маркетингу деякий час не використовувалась.

Зі зростання мережі Інтернет зростали і масштаби спам-кампаній. Після 2000 року кількість нав'язливих розсилок стрімко зросла, досягнувши піку в 2008 році, коли такий контент становив більше 90% всього трафіку електронної пошти. Більше того, такі розсилки не просто поширювали небажані оголошення, фішингові посилання та інший шкідливий вміст, але й небезпечні сімейства шкідливих програм, що зробило їх серйозною загрозою для кібербезпеки.

Вендори рішень для кібербезпеки та розробники програмного забезпечення створили рішення для захисту від спаму, більшість з яких базуються на машинному навчанні та здатні знаходити цей вид повідомлень. Урядовці також розробили розробили законодавчу базу для протидії спаму, завдяки яким його розповсюдження стало незаконним та навіть піддається судовому переслідуванню.

У 2008 році був закритий хостинг-провайдер McCol з Каліфорнії, тому що він розміщував пристрої, відповідальні за надсилання небажаних комерційних розсилок. Підраховано, що сервери McColo були відповідальними за надсилання трьох чвертей усіх спам-повідомлень у світі.

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Електронна пошта, спам, повідомлення, реклама, додаток, повідомлення, лист, вірус, шкідливий, небезпечний, загроза, атака, бот, злом,

6. What is the name of the risk management group?
7. In what situations should risk assessment be effective?
8. What are the useful tasks?
9. Who captures the vulnerabilities, threats, plausibility and impact elements within the training
10. How to decipher the abbreviation NIST?

Task 8. Complete the following sentences using the text.

1. Pre-assessment includes ___ _____ ___ _____, identification of relevant actors and stakeholders, and captures perspectives on risk.
2. Note that the ordering of actions in the NIST approach puts threat identification before vulnerabilities, which presupposes that all threats ____ ___ _____ and mapped to vulnerabilities.
3. While not wishing to reproduce the whole list here, we provide ___ _____ for the purposes of comparison.
4. Threat modelling, of course, cannot guarantee that all failures can be predicted, but the _____ _____ _____continual assessment of evolving threats if time and resources allow.
5. The approach is designed ___ _____ _____ _____assessment and could be performed in-house possibly resulting in a lower cost than a consultant-led risk assessment.
6. It also involves defining assumptions and constraints on elements such as resources required and _____ _____that need to inform the risk assessment.
7. Appraisal includes ____ _____ _____ _____and consequences of risk (including risk concern), developing a knowledge base of risks and mitigation options (e.g., preventing, sharing etc).
8. Cutting across all four is communication, engagement and _____ _____through open and inclusive dialogue.

9. Management processes include deciding on the risk management plan and _____ _____ _____ ____including risk tolerance (accepting, avoiding, mitigating, sharing, transferring).
10. Characterisation involves ___ _____ _____, making a judgment about the significance and tolerance of the risks.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English

Поява та управляння кібер-ризиками

Поява поняття «кібер-ризику» стало першим кроком на шляху розуміння бізнесом важливості кібербезпеки. Саме «кібер-ризик» означає ризик фінансових втрат (прямих і непрямих), повної або часткової зупинки діяльності, а також шкоди репутації організації або приватної особи. Часто після цього визначення додають щось на кшталт «в результаті порушення роботи інформаційних сервісів і систем». Це не зовсім вірно, і ми зараз пояснимо різницю між таким підходом до роботи з ризиками та нашим.

Саме поняття кібербезпеки набагато ширше інформаційних систем і ресурсів. Воно включає в себе всі ресурси компанії або організації, в тому числі, співробітників, підрядників і партнерів. Будь-яка сфера діяльності або активності, яка може притягнути загрозу реалізації вищезазначених ризиків, формує повне охоплення вже кібер-ризиків.

Управління кібер-ризиками – це фундамент для будь-якої дії у сфері безпеки, чи то впровадження систем або інструментів, або побудова процесів і впровадження правил і політик. Проекти з управління ризиками часто недооцінюють і не відокремлюють. Хоча саме грамотне визначення та

миттєві та текстові повідомлення (SMS), соціальні медіа або навіть голосову пошту.

Один з найбільш поширених способів розповсюдження небажаного контенту – використання ботнет-мереж, великої кількості інфікованих «зомбі» пристроїв. Іноді так звані «листи щастя» (повідомлення із закликом поширити його серед друзів, обіцяючи за це гроші/здоров'я/кохання чи навпаки невдачі) та Інтернет-розіграші також вважаються спамом, хоча вони й відрізняються тим, що найчастіше надсилаюся з добрими намірами.

Напевно, кожен шанувальник британського комедійного телевізійного шоу «Монті Пайтон» знає звідки походить термін спам. У одному із скетчів 1970 року два гості замовляють їжу в кафе та помічають, що майже кожна страва в меню містить SPAM® – тип консервованого м'яса. Незважаючи на те, що один з них не бажає їсти цю страву, незабаром стає зрозуміло, що уникнути цей інгредієнт, як і небажаних повідомлень електронної пошти, майже неможливо.

Як розпізнати спам?

Якщо повідомлення електронної пошти або будь-яка інша форма масової комунікації є небажаною та вводить в оману, можливо, вона є спамом.

PS: Якщо це слово написане великими літерами на баночці, найімовірніше це відомий американський харчовий продукт, який складається з вареної шинки та свинини.

Як забезпечити захист від спаму?

Ніколи не публікуйте свою електронну адресу на публічних веб-сайтах та сервісах. Якщо її все-таки необхідно вказати, робіть це з обережністю. Ви також можете створити одноразову адресу електронної пошти, яку можна використовувати для оглядів новин або підписок.

Також використовуйте рішення, які володіють функціями для виявлення небажених повідомлень, серед яких наявна перевірка листа на спам.

1. Learn how to detect spam by looking out for the following , all illustrated with recent examples from my personal email account.

2. Messaging spam: Like spam, but quicker.

3. Anyone who's spent more than a handful of seconds on the has encountered spam.

4. As you read through this section, pay close to the actual email addresses in these examples.

5. Mobile spam: It's spam in form.

6. You can over to our handy Hack Check tool and see if any of your have been leaked.

7. The is trying to exploit an SEO mechanic known as "backlinking" to drive traffic to their page.

8. If the definition of spam is unsolicited , spamming is the act of sending these messages, and a person who engages the practice is a spammer.

9. It's annoying, it's usually , it's sent to loads of people, and it's coming whether you asked for it or not.

10. But when it comes to the variety, there's an equally diverse menu available.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Що таке спам?

Спам – це небажані повідомлення у будь-якій формі, які надсилаються у великій кількості. Найчастіше спам надсилається у формі комерційних електронних листів, надісланих на велику кількість адрес, а також через

управління кібер-ризиками дозволяє розподілити раціонально бюджет на кібербезпеку і грамотно підготуватися до атак і загроз заздалегідь.

Передумов для формалізації процесів управління кібер-ризиками кілька:

- оцифровка (або «діджиталізація») сучасного бізнесу. Вже практично не залишилося галузей, які не залучені в кіберпростір, і розмір компаній вже також не має значення;
- потрапляння самої людини до охоплення застосування кібер-ризиків. Людина навіть сама по собі вже є інформаційним активом, який необхідно захищати;
- зростання залежності областей безпеки одна від одної. Наприклад, фізичної безпеки від інтернету речей;
- потреба топ-менеджерів у простому й зрозумілому інструменті оцінки безпеки та її розвитку.

У світі існує безліч методологій побудови процесів управління ризиками і первинної оцінки ризиків. Coras, CRAMM, PRISM, RiskWatch, OCTAVE – це лишень мала частина переліку існуючих практичних методик. Є уніфіковані методики, є галузеві. Досвідченому консультанту не важко вибудувати процеси оцінки й управління кібер-ризиками в рамках будь-якої з них. Базові принципи єдині, а їхній логічний ряд збудовано єдиним правильним ланцюжком до появи інформаційних технологій.

Якщо ви ніколи раніше не були дотичні до управління ризиками, в компанії не знають, що таке карта ризиків і для чого вона потрібна, то варто починати з аналізу ризиків. Його проводять навіть за умови впроваджених і налагоджених процесів управління, тому що кібер-ризики – субстанція дуже жива і змінюються вони досить часто і сильно. Під час первинної оцінки ризиків необхідно в першу чергу визначити цілі управління кібербезпекою компанії. Після цього необхідно визначити критично важливі елементи, які впливають на ключові бізнес-процеси компанії. Кожен ризик, у класичному розумінні, оцінюється за двома параметрами: ймовірності й потенційного

збитку. Виходячи з цих кількісних показників формується карта ризиків і їхній пріоритет. Таку оцінку необхідно проводити регулярно, розширюючи карту ризиків, щоб охопити якомога більше потенційних ризиків для компанії.

На підставі оцінки кібер-ризиків проводиться їхня пріоритезація для бізнесу. Як правило, це показник фінансовий, який зрозумілий представникам топ-менеджменту і бізнес підрозділів. І далі починається найцікавіше: робота з ризиками. Тобто, кожен ризик після оцінки підлягає аналізу, щоб опрацювати заходи роботи з ним. Є класичний набір таких заходів: мінімізація, прийняття, ухилення, перекладання і диверсифікація. Проте в різних методиках можуть виникати нові терміни або інструменти. Завдання цього етапу робіт полягає у виборі правильного інструменту управління для кожного ризику (інструмент може бути переглянутий згодом та змінений). Наприклад, іноді компанії беруть ризик втрати клієнта, розуміючи, що фінансово їм буде невигідно боротися за нього. Так і в кібербезпеці може виявитися, що захист якогось ресурсу або активу є недоцільним, отже простіше застрахувати його втрату або компрометацію.
https://spilno.org/article/kiber-ryzyky-yak-rozumity-ta-upravlyaty

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Низка методів, керівні прицнипи, правдоподібність, рейтинговий список, оцінка ризику, експертна група, зацікавлені сторони, контекстне налаштування, виявлення вразливостей, ймовірні загрози, список загальноприйнятих компонентів, інклюзивний діалог, системні перспективи, способи його реалізації, прийняття, уникнення, пом’якшення, керуючий, експертна група.

If someone gets control of your email account, you might find yourself inundated with spam. You can pop over to our handy Hack Check tool and see if any of your passwords have been leaked.

Learn how to detect spam by looking out for the following types of messages, all illustrated with recent examples from my personal email account. Because my email service automatically blocks some elements of spam emails, many images in the emails are not visible.

As you read through this section, pay close attention to the actual email addresses in these examples. Notice how they’re all very long and largely composed of random letters and numbers. This an intentional act on the spammer’s part which helps obfuscate their identity.

Джерело: https://www.avast.com/c-spam

III. Post-reading activities.

Task 7. Answer the following questions.

1. Are there any spam links?
2. Where can you see spam links?
3. What is the other name for spam?
4. What is the third most common spams?
5. Is it possible to recognize spam messages from a regular message?
6. Is there spam in online games?
7. Is there spam in ads?
8. Is it easy to recognize spam?
9. Do you know how to detect spam?
10. How can spam get on your computer?

Task 8. Complete the following sentences using the text.

Email spam: Your garden-variety spam. It clogs up your inbox and distracts you from the emails you actually want to read. Rest assured, it's all extremely ignorable.

SEO spam: Also known as spamdexing, this is the abuse of search engine optimization (SEO) methods to improve search rankings for the spammer's website. We can divide SEO spam into two broad categories:

◦ Content spam: Spammers cram their pages full of popular keywords, usually unrelated to their website, to try and rank their site higher in searches for those keywords. Others will rewrite existing content to make their own pages seem more substantial and unique.

◦ Link spam: If you've come across a blog comment or forum post that's filled with irrelevant links, you've encountered link spam. The spammer is trying to exploit an SEO mechanic known as "backlinking" to drive traffic to their page.

Social networking spam: As the internet grows ever more social, spammers are quick to take advantage, spreading their spam via fake "throwaway" accounts on popular social networking platforms.

Mobile spam: It's spam in SMS form. In addition to spammy text messages, some spammers also utilize push notifications to draw your attention to their offers.

Messaging spam: Like email spam, but quicker. Spammers blast their messages out on instant messaging platforms including WhatsApp, Skype, and Snapchat.

How to recognize spam

Regardless of how it reaches you – as email spam, social network spam, or one of the others – most spam fits neatly into one of a handful of "genres". Once you get an idea of what most spam looks like, it's easy to recognize it when it comes your way.

Unit 4. Cyber risk assessment and management

I. Pre-reading activities.

Task 1. How do you understand the statement: *"A key to achieving success is to assemble a strong and stable management team"* (*Vivek Wadhwa)*. **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What do you think cyber security means?
2. Have you ever heard about cyber risk?
3. Who do you think is responsible for the cyber security of citizens?

Task 3. Try to guess the meaning of the following words.

Digital, underpin, framework, cooperation, assessment, preparedness, risk –taking situation.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

We will begin with high level definitions of some of the 1). foremost positions on risk. Cyber security is such 2). a rapidly evolving domain that we must accept that we cannot be fully cyber secure. The Potomac Institute for Policy Studies provides a framework for studying cyber readiness along with 3). a country-specific profile for a range of nations. Like much of the risk assessment process, there is no 4). one-size solution for all endeavors. For instance, 5). incorporating social and economic drivers…it is absolutely crucial for effective risk governance to include the wider 6). stakeholder view.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1). evidence	a). займати певне місце
2). aggregate	b). поширюваний
3). perceptions	c). сукупність
4). pervasive	d). висувати на передній план
5). rank	e). доказ
6). highlight	f). сприйняття

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. Is digital technology necessary for humanity today?
2. Which human decision-based tasks are being replaced by automated technologies?
3. For whom is cyber security risk assessment and management important?

Cyber risk assessment and management

Digital technology is becoming evermore pervasive and underpins almost every facet of our daily lives. With the growth of the Internet of Things, connected devices are expected to reach levels of more than 50 billion by 2022. Further, human decision-based tasks such as driving and decision-making are being replaced by automated technologies, and the digital infrastructures that we are increasingly reliant upon can be disrupted indiscriminately as a result of, for example, ransomware. Cyber security risk assessment and management is,

Spamming

What is spamming?

Anyone who's spent more than a handful of seconds on the internet has encountered spam. It's seemingly an inseparable part of the internet experience, something we accept as normal. But how can we define spam? What makes spam emails different from others? In terms of the internet, what does spam mean?

The answer is that spam is always unrequested. It's annoying, it's usually promotional, it's sent to loads of people, and it's coming whether you asked for it or not. If you've signed up for a marketing newsletter and later gotten sick of it, that's unfortunate, but it isn't spam.

If the definition of spam is unsolicited bulk messages, spamming is the act of sending these messages, and a person who engages the practice is a spammer. Most of the time, spamming is commercial in nature, and though the spam is bothersome, it isn't necessarily malicious or fraudulent (though it can be).

Why is it called spam?

The use of the term "spam" to describe this type of invasive blanket-messaging is a reference to a Monty Python skit. In it, a group of diners (clad in Viking costumes, no less) loudly and repeatedly proclaim that everyone must eat Spam, regardless of whether they want it or not. It's similar to how an email spammer will flood your inbox with their unwanted messages.

When spelled with a capital S, "Spam" refers to the canned pork product that the above-mentioned Vikings love. Use a lowercase S to discuss the endless flood of emails and other messages that you never asked for.

What kinds of spam are there?

You can fry it, bake it, scramble it with eggs, eat it on a sandwich, or even serve it with rice and seaweed. But when it comes to the electronic variety, there's an equally diverse menu available. Here's a short list of what you might expect in the wide world of spam:

5. An early example of nonprofit fundraising bulk posting via Usenet also occurred in 1994 on behalf of CitiHope, an NGO attempting to raise funds to rescue children at risk during the Bosnian War.

6. Email spam, also known as unsolicited bulk email (UBE), or junk mail, is the practice of sending unwanted email messages, frequently with commercial content, in large quantities.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1). spam	a). поширювати
2). email	b). вихідні повідомлення
3). content	c). копії
4). trigger	d). кібербезпека
5). Spam filters	e). брандмауери
6). bot	f). корисне навантаження
7). firewalls	g). жертва
8). bot	e). спам-фільтри

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. Are all spams fraudulent and harmful?
2. What does the word spam mean in Monty Python's scene?
3. Is there spam on social media?

therefore, a fundamental special case that everyone living and working within the digital domain should understand and be a participant in it.

There are a number of global standards that aim to formalise and provide a common framework for cyber risk assessment and management, and, in this section, we will study some of them. We will begin with high level definitions of some of the foremost positions on risk. The United Kingdom was ranked first in the 2018 Global Cybersecurity Index (GCI), a scientifically grounded review of the cyber security commitment and situation at a global country-by-country level. The review covers five pillars: (i) legal, (ii) technical, (iii) organisational, (iv) capacity building, and (v) cooperation – and then aggregates them into an overall score. As the lead nation in the GCI, the technical authority for cyber security, the UK National Cyber Security Centre (NCSC) has published guidance on risk management. Importantly, the NCSC is clear that there is no one-size-fits-all for risk assessment and management. Indeed conducting risk assessment and management as a tick-box exercise produces a false sense of security, which potentially increases the Vulnerability of the people impacted by risk because they are not properly prepared. Cyber security is such a rapidly evolving domain that we must accept that we cannot be fully cyber secure. However, we can increase our preparedness. The Potomac Institute for Policy Studies provides a framework for studying cyber readiness along with a country-specific profile for a range of nations (inc. USA, India, South Africa, France, UK) and an associated cyber readiness index.

What is risk governance and why is it essential? Risk assessment and developing mitigation principles to manage risk is only likely to be effective where a coordinated and well communicated governance policy is put in place within the system being managed. Millstone proposed three governance models:

- Technocratic: where policy is directly informed by science and evidence from domain expertise.

- Decisionistic: where risk evaluation and policy are developed using inputs beyond science alone. For instance, incorporating social and economic drivers.
- Transparent (inclusive): where context for risk assessment is considered from the outset with input from science, politics, economics and civil society. This develops a model of "pre-assessment" – that includes the views of wider stakeholders – that shapes risk assessment and subsequent management policy. None are correct or incorrect.

There is a fine balance between the knowledge and findings of scientific experts, and perceptions of the lay public. While the technocratic approach may seem logical to some risk owners who work on the basis of reasoning using evidence, it is absolutely crucial for effective risk governance to include the wider stakeholder view.

Rohrmann and Renn's work on risk perception highlights some key reasons for this. They identify four elements that influence the perception of risk:

- intuitive judgment associated with probabilities and damages;
- contextual factors surrounding the perceived characteristics of the risk (e.g., familiarity) and the risk situation (e.g., personal control);
- semantic associations linked to the risk source, people associated with the risk, and circumstances of the risk-taking situation;
- trust and credibility of the actors involved in the risk debate.

These factors are not particularly scientific, structured or evidence-based but, as noted by Fischoff, such forms of defining probabilities are countered by the strength of belief people have about the likelihood of an undesirable event impacting their own values. Ultimately, from a governance perspective, the more inclusive and transparent the policy development, the more likely the support and buy-in from the wider stakeholder group – including lay people as well as operational staff – for the risk management policies and principles. There are several elements that are key to successful risk governance. Like much of the risk assessment process, there is no one-size solution for all endeavors. However, a

Unit 19. Spamming

I. <u>Pre-reading activities.</u>

Task 1. How do you understand the word: "spam". Translate it into Ukrainian.

Task 2. Discuss the following questions.

1. Have you ever encountered spam?
2. What makes spam emails different from others?
3. How do we call the person who deals with spam?

Task 3. Try to guess the meaning of the following words.

SEO spam, link spam, attack, system, online, message, bot, network (VPN), IP Address.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. The easiest way to avoid <u>spam filters</u> is by carefully choosing the words you use in your email's subject line.

2. We've compiled a list of 202 <u>spam trigger words</u> you should avoid the next time you sit down to write an email subject line.

3. There is nothing wrong with urging your reader to take action, but spam filters often <u>penalize</u> emails with subject lines that create unnecessary urgency and pressure.

4 A type of software application or script that performs tasks on command, allowing an attacker to take complete control <u>remotely of an affected computer</u>.

вікна, Ви можете дозволити їх у кожному конкретному випадку. Якщо непотрібне Вам вікно все ж з'явилось, не натискайте кнопку "скасувати", такі кнопки часто призводять до фішинг-сайтів, замість цього натисніть на маленьке "х", щоб його закрити.

7. Ніколи не видавати особисту інформацію – як правило, Ви ніколи не повинні ділитися особистою, або фінансово чутливою інформацією через Інтернет. Якщо в цьому є потреба, завжди намагайтесь самостійно перейти на першоджерело, перевіривши всі фактори, що це саме той ресурс, який Вам потрібен.

Це тільки мінімальний список простих правил, які мають стати звичкою для користувачів у сучасному світі. Більш складні фішингові електронні листи виконують прихований код, якщо пошта просто відкривається на цільовому комп'ютері.

Одним з варіантів зменшення ризиків – є використання спеціалізованих програмних чи програмно-апаратних комплексів від лідируючих компаній в галузі інформаційної/мережевої безпеки.

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Фішинг, соціальна інженерія, хакерські атаки, шахрайство, кіберпростір, кібер атака, джерело інформації, хакери, шукати в інтернеті, персональні дані, вкрасти персональні дані, шкідливе влкадення, фішингові сайти, кібератака, фішинг-атаки, видаляти програму, надійні паролі, зареєструватись, скачати антивірус, роздрукувати, додаток, ноутбук, персональний комп'ютер, вірус, інформаційні технології, злом, вспливаючі реклами, Троянський кінь.

major principle is ensuring that the governance activity (see below) is tightly coupled with everyday activity and decision-making. Cyber risk is as important as health and safety, financial processes, and human resources. These activities are now well established in decision-making. For instance, when hiring staff, the HR process is at the forefront of the recruiter's activity. When travelling overseas, employees will always consult the financial constraints and processes for travel. Cyber security should be thought of in the same way – a clear set of processes that reduce the risk of harm to individuals and the business. Everyone involved in the daily running of the system in question must understand that, for security to be effective, it must be part of everyday operational culture. The cyber risk governance approach is key to this cultural adoption.

III. Post-reading activities.

Task 7. Answer the following questions.

1. What does GCI mean?
2. What is the place of The United Kingdom in the 2018 Global Cybersecurity Index?
3. Which five pillars does the review cover?
4. What has the UK National Cyber Security Centre (NCSC) published ?
5. In what way can we increase our readiness in cyber security?
6. Under what conditions can risk assessment and developing mitigation principles be effective?
7. What are three governance models?
8. What is Rohrmann and Renn's work about?
9. What four elements that influence the perception of risk do they (Rohrmann and Renn) identify?
10. Why the cyber risk governance approach is key to this cultural adoption?

Task 8. Complete the following sentences using the text.

1. What is risk _____ and why is it essential?
2. Digital technology is becoming evermore _____ and underpins almost every facet of our daily lives.
3. There are several elements that are _____ to successful risk governance.
4. They identify four elements that influence the _____of risk.
5. _____ is as important as health and safety, financial processes, and human resources.
6. Like much of the risk assessment process, there is no _____ for all endeavors.
7. However, we can increase our _____.
8. These activities are now well established in _____.
9. The cyber risk governance _____ is key to this cultural adoption.
10. As the lead nation in the GCI, the technical authority for cyber security, the UK National Cyber Security Centre (NCSC) has published _____ on risk management.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English

Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними

В останні кілька років суттєво збільшилася кількість кібер-атак на світові та українські організації. Метою хакерів стають не тільки державні

на випадкових емейлах чи повідомленнях у месенджерах – може бути не дуже гарною ідеєю. Наведіть курсор на посилання, в яких Ви не впевнені, і перевірте чи справді Вони ведуть туди, куди повинні вести? Фішинг-листи можуть маскуватися під відому вам компанію, переходячи за посиланням, Ви навіть побачите сайт схожий на справжній, електронні листи можуть містити навіть Ваше ім'я, краще перейдіть до безпосередньо до джерела самостійно, не натискаючи на потенційно небезпечне посилання.

4. Перевірте безпеку сайту – природно бути трохи обережним у наданні конфіденційної фінансової інформації в мережі Інтернет. Поки Ви перебуваєте на захищеному веб-сайті, Ви не повинні мати жодних проблем. Перш ніж надсилати будь-яку інформацію, переконайтеся, що URL-адреса сайту починається з "https", а біля адресного рядка має бути значок закритого замка. Перевірте також сертифікат безпеки сайту, з ним не має бути ніяких проблем, він має відповідати тому ресурсу, на якому Ви знаходитесь. Якщо Ви отримаєте повідомлення про те, що певний веб-сайт може містити шкідливі файли, не відкривайте цей ресурс. Ніколи не завантажуйте файли з підозрілих електронних листів чи веб-сайтів. Навіть пошукові системи можуть показувати певні посилання, що може призвести користувачів до фішинг-сторінки, яка пропонує продукти з низькою ціною. Якщо користувач здійснює покупки на такому веб-сайті, інформацію про кредитну карту отримають кіберзлочинці.

5. Досліджуйте техніки фішингу – на сьогодні багато ресурсів в мережі описують методи, які застосовуються злочинцями, дізнавшись про них раніше, Ви маєте шанс не стати жертвою одного з них. Фахівці, що відповідають за інформаційну безпеку в компаніях, постійно мають проводити навчання колег, та імітувати фішинг для всіх користувачів в компанії.

6. Будьте обережні зі спливаючими вікнами – спливаючі вікна часто маскуються як законні компоненти веб-сайту. Хоча вони занадто часто є фішинговими. Багато популярних браузерів дозволяють блокувати спливаючі

щоб замаскувати комунікації або веб-сторінки під надійне джерело. По суті, фішингові атаки покладаються на методи, що мають викликати довіру, а також на технологічні хитрощі для досягнення своїх цілей.

На відміну від них, цільовий фішинг спрямований на конкретну особу або компанію. Подібні атаки, як правило, застосовують наступні методи та технології: клонування сторінки входу в корпоративні інтранет-мережі, використання особистої інформації, зібраної заздалегідь для збільшення ймовірності успіху, та інші. Цільовий фішинг проти вищих керівників компаній називаються китобійним.

Метод китобійного фішінгу також називається «шахрайство з генеральним директором», адже фішингові листи маскуються як такі, що походять від генерального директора. За словами експертів, ці атаки на базі соціальної інженерії є дуже руйнівними, оскільки листи електронної пошти виглядають вельми реалістично і жертви нерідко добровільно надсилають гроші.

Тож спочатку зловмисники ідентифікують цілі, спостерігають за ними, а потім видурюють гроші за допомогою електронної пошти. Мета шахрая – переказати кошти на свої банківські рахунки, зазвичай – в азійських банках, які потім спорожняються. Малі та середні підприємства є особливо вразливими для такого шахрайства, адже там менше бюрократичних перепон в комунікаціях між

1. Регулярно перевіряйте свої облікові записи в Інтернеті – якщо Ви деякий час не відвідуєте Інтернет-акаунт, хтось уже може ним користуватись. Візьміть за правило регулярно змінювати свої паролі. Завжди контролюйте інформацію про рух коштів на Вашому рахунку, щоб бути впевненим, що жодні шахрайські операції не здійснювались.

2. Постійно оновлюйте веб-браузер – у всіх популярних веб-браузерів постійно виходять оновлення безпеки, не нехтуйте ними.

3. Подумайте, перш ніж натиснути! – нормально переходити на посилання, знаходячись на надійних веб-ресурсах, але клацати на посилання

інститути і підприємства, а й приватний сектор (малий та середній бізнес), адже комп'ютерні системи, які використовують у своїй діяльності організації малого та середнього бізнесу, є уразливими та мають багато прогалин. Щодня тисячі малих підприємств в усьому світі піддаються кібер-атакам. Крадії намагаються вкрасти інформацію та гроші, або втрутитися в бізнес. Наприклад, лише у Великій Британії в 2014 році 60% організації малого бізнесу відчули вплив кібер–ризиків (пережили кібер-атаки, в результаті яких втратили приблизно від 65000 фунтів стерлінгів до 115 000 фунтів стерлінгів).

Згідно із звітом про ризики кібербезпеки Cybersecurity Venturesreport, до 2019 року бізнес у світі буде стикатися з атаками кожні 14 секунд. До 2021 року збитки від загроз кібербезпеки будуть оцінюватися в 6 трлн дол. Крім збільшення кількості кібератак, буде зростати й рівень складності кіберзлочинів. Кібер-інциденти продовжують рух угору в рейтингу і зараз є другим за важливістю ризиком для компаній усього світу (40%) в цьому рейтингу. З огляду на мінливу природу кіберризику, а також зростання числа кібер-інцидентів, ризик займає один із верхніх рядків серед найважливіших ризиків у світі. Такими є ключові висновки Барометра ризиків Allianz, щорічно публікується Allianz Global Corporate & Specialty (AGCS). Звіт ґрунтується на думці 1911 експертів із ризик-менеджменту з 80 країн світу.

А лише п'ять років тому кібер-ризики знаходилися лише на 15 місці. Такі загрози, як порушення даних, хакерські атаки або ж перерви у виробництві внаслідок кібер-інциденту підтверджують, що це є головним ризиком для бізнесу на Американському континенті і другим за значущістю ризиком у Європі та Азіатсько-Тихоокеанському регіоні.

Кібер-ризики є найбільш недооціненими ризиками в довгостроковій перспективі в Україні.

Яскравим прикладом цього є те, що у 2017 році під час кібератаки вірусу Petya постраждали понад 1500 компаній, а 13 тис комп'ютерів були заражені. За рік український бізнес втратив від кібератак мільярди гривень.

За результатами опублікованих наукових та практичних робіт фахівців, а також даних таблиці 1 ми згрупували кібер-ризики за такими ознаками, як: 1) втрата або крадіжка носіїв інформації та мобільних пристроїв; 2) доступ сторонніх осіб до конфіденційної інформації за допомогою вразливих хмарних сховищ; 3) ненавмисне розголошення співробітниками конфіденційної інформації; 4) навмисні дії співробітників (інсайдерів); 5) неконтрольоване копіювання даних співробітниками.

Отже, кібер-шантаж, фішингові атаки, зломи особистих пристроїв і крадіжка даних – це сучасні ризики для діяльності малих та середніх підприємств. Часто малий та середній бізнес вважають більш легкою мішенню порівняно з великими компаніями. За даними компанії Symantec, 75% організацій малого та середнього бізнесу стали жертвами фішингових атак. Серед великих компаній постраждало тільки 35%.

У світлі зростання кількості і серйозності цього питання організації малого та середнього бізнесу змушені внести до свого списку ще одну небезпеку для бізнесу, на яку раніше закривали очі, – це кібер-ризики.

Source: https://chmnu.edu.ua/wp-content/uploads/2019/07/Vinnikova-I.I.-Marchuk-S.V..pdf

Task 11. Give the English equivalents of the Ukrainian words and word combinations.

Державні інститути, малий та середній бізнес, уразливий, втрутитися в бізнес, вплив кібер–ризиків, стикатися з, збитки, рівень складності, мінлива природа, кібер-інциденти, щорічно публікуватись, ґрунтуватись на, порушення даних, недооцінений, яскравим прикладом цього є, проведено аналіз, конфіденційна інформація, вразливий, неконтрольоване копіювання даних, фішингові атаки, мішень.

Task 8. Complete the following sentences using the text.

1. Some _____ _____ aim to get login information from, or infect the computers of, specific people.
2. Gathering enough _____ to trick a really high-value target might take time, but it can have a surprisingly high payoff.
3. The term arose in the mid-1990s among hackers aiming to trick AOL users into giving up their _____ _____.
4. The _____ can now access the victim's account.
5. Nearly a third of all breaches in the past year involved _____, according to the 2019 Verizon Data Breach Investigations Report.
6. In fact, they downloaded keyloggers onto the executives' computers — and the scammers' success rate was 10%, snagging almost _____ victims.
7. Like a lot of spam, these types of _____ _____ aim to get the victim to infect their own computer with malware.
8. _____ dedicate much more energy to tricking those victims, who have been selected because the potential rewards are quite high.
9. When attackers try to craft a message to appeal to a specific individual, that's called _____ _____.
10. For cyber-espionage attacks, that number jumps to _____.

Task 10. Translate from Ukrainian into English.

Фішинг існує з початку створення мережі Інтернет і техніки та постійно вдосконалюється. Кількість атак з використанням фішингу буде тільки зростати, що дасть можливість зловмисникам отримувати великі прибутки. В сучасному світі, треба взяти за правило декілька речей, що допоможуть знизити ризик стати жертвою фішинг-атаки.

Фішинг — це метод соціальної інженерії, що дозволяє шахрайським шляхом отримувати інформацію, яку потім можна використовувати для доступу до пристроїв або мереж. Цей тип атаки застосовує певні технології,

Whaling

Whale phishing, or whaling, is a form of spear phishing aimed at the very big fish – CEOs or other high-value targets. Many of these scams target company board members, who are considered particularly vulnerable: they have a great deal of authority within a company, but since they aren't full-time employees, they often use personal email addresses for business-related correspondence, which doesn't have the protections offered by corporate email.

Gathering enough information to trick a really high-value target might take time, but it can have a surprisingly high payoff. In 2008, cybercriminals targeted corporate CEOs with emails that claimed to have FBI subpoenas attached. In fact, they downloaded keyloggers onto the executives' computers – and the scammers' success rate was 10%, snagging almost 2,000 victims.

Джерело:https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

III. Post-reading activities.

Task 7. Answer the following questions.

1. Name the most common examples of a phishing attack.
2. What is one of the most consequential phishing attacks in history?
3. Why is it called phishing?
4. What is CEO?
5. How do you stay safe online?
6. What brands are always attacked by scammers?
7. What is whaling?
8. How can you be cybersmart to stay safe?
9. What to do when you've been phished?
10. What does «phreaking» mean?

Unit 5. Hardware attacks

I. Pre-reading activities.

Task 1. How do you understand the statement: "*Hardware and software should be treated together, integrated with cybersecurity early and frequently"* (Linda Rawson). **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. Which tools allow developers to assess its security?
2. Into what groups are the attacks divided?
3. What is a real threat for algorithms proven secure mathematically?

Task 3. Try to guess the meaning of the following words.

Physical attacks, hardware-targeted soware attacks, electromagnetic emissions, Encryption Standard, SSD disks, hardware, software, Rowhammer attack, software attack, Dynamic Voltage and Frequency Scaling.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

Unfortunately, those tools cannot consider the 1). interaction of the computing unit with its physical environment. 2). Observation attacks 3). Side-channel analyses (SCA) are 4). physical attacks based on the 5). observation of the circuit behavior during a computation. The most classic leakages are timing, 6). power consumption, and 7). electromagnetic emissions (EM).

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1). hardware	a). програмне забезпечення
2). interaction	b). низькошарові атаки
3). amplitude	c). атака ускладнення (збурення)
4). software	d). взаємодія
5). low-layer attacks	e). діапазон
6). perturbation attacks	f). апаратне забезпечення

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. Why are the physical attacks a real threat?
2. What is the Rowhammer attack?
3. What is the function of softaware-based attacks?

Hardware attacks

When discussing the security of an algorithm, numerous mathematical tools allow developers to assess its security. Unfortunately, those tools cannot consider the interaction of the computing unit with its physical environment. Physical attacks are a real threat, even for algorithms proven secure mathematically. These attacks can be classified as observation attacks, perturbation attacks, and a new field known as hardware-targeted soware attacks. The first two assume the insider attacker model i.e., the device is under the attacker’s control, while the last one assumes the outsider model. The outsider model requires fewer hypotheses for the attacker and thus can be considered as more dangerous.

2017 it was estimated that 93% of phishing emails contained ransomware attachments.

Phishing emails can be targeted in several different ways. As we noted, sometimes they aren't targeted at all; emails are sent to millions of potential victims to try to trick them into logging in to fake versions of very popular websites. Iron scales has tallied the most popular brands that hackers use in their phishing attempts.

Of the 50,000-plus fake login pages the company monitored, these were the top brands attackers used:

- PayPal: 22%
- Microsoft: 19%
- Facebook: 15%
- eBay: 6%
- Amazon: 3%

Other times, attackers might send "soft targeted" emails at someone playing a particular role in an organization, even if they don't know anything about them personally. Some phishing attacks aim to get login information from, or infect the computers of, specific people. Attackers dedicate much more energy to tricking those victims, who have been selected because the potential rewards are quite high.

Spear phishing

When attackers try to craft a message to appeal to a specific individual, that's called spear phishing. (The image is of a fisherman aiming for one specific fish, rather than just casting a baited hook in the water to see who bites.) Phishers identify their targets (sometimes using information on sites like LinkedIn) and use spoofed addresses to send emails that could plausibly look like they're coming from co-workers. For instance, the spear phisher might target someone in the finance department and pretend to be the victim's manager requesting a large bank transfer on short notice.

Apple's iCloud servers, but was in fact the product of a number of successful phishing attempts.

• In 2016, employees at the University of Kansas responded to a phishing email and handed over access to their paycheck deposit information, resulting in them losing pay.

Types of phishing

If there's a common denominator among phishing attacks, it's the disguise. The attackers spoof their email address so it looks like it's coming from someone else, set up fake websites that look like ones the victim trusts, and use foreign character sets to disguise URLs.

That said, there are a variety of techniques that fall under the umbrella of phishing. There are a couple of different ways to break attacks down into categories. One is by the purpose of the phishing attempt. Generally, a phishing campaign tries to get the victim to do one of two things:

• Hand over sensitive information. These messages aim to trick the user into revealing important data — often a username and password that the attacker can use to breach a system or account. The classic version of this scam involves sending out an email tailored to look like a message from a major bank; by spamming out the message to millions of people, the attackers ensure that at least some of the recipients will be customers of that bank. The victim clicks on a link in the message and is taken to a malicious site designed to resemble the bank's webpage, and then hopefully enters their username and password. The attacker can now access the victim's account.

• Download malware. Like a lot of spam, these types of phishing emails aim to get the victim to infect their own computer with malware. Often the messages are "soft targeted" — they might be sent to an HR staffer with an attachment that purports to be a job seeker's resume, for instance. These attachments are often .zip files, or Microsoft Office documents with malicious embedded code. The most common form of malicious code is ransomware — in

Observation attacks Side-channel analyses (SCA) are physical attacks based on the observation of the circuit behavior during a computation. They exploit the fact that some physical quantities depend on intermediary values of the computation in the device. This is the so-called information leakage. The most classic leakages are timing, power consumption, and electromagnetic emissions (EM). SCA are threats for all standard cryptosystems such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA cryptosystem, Elliptic Curve Cryptography (ECC) and for critical applications not using cryptography, e.g. PIN verification. SCA can also be used to reverse engineer algorithms.

Perturbation attacks Fault attacks are now a well-known class of physical attacks where a device undergoes a modification of physical parameters in order to obtain an incorrect behavior. Most classical fault injection means are power glitches, clock glitches, laser pulses, and electromagnetic pulses. Fault attacks have been shown extremely efficient against cryptography, e.g. the Bellcore attack allows any fault, at the correct time, on an RSA-CRT signature to recover the secret. What fault can be achieved and what is the fault model is an active area of research.

This class of attack is chip dependent, i.e. what has been learned of a SoC is not valid for other chips even if they are highly similar (same core). The success of the attack relies essentially on the experiment set up due to the large amountof parameters (type of the EM probe, distance of the probe on the circuit, form and amplitude of the EM pulse, etc.). Another challenge in this class of attacks is the effects observability. To understand the precise effect, one has to explore the internal state of the chip which is oen not available. Most of the countermeasures are related with either temporal or spatial redundancy. The cost of such a redundancy is not affordable for low end devices. Research is focusing on lightweight redundancy to ensure the integrity of the execution.

Hardware-targeted software attacks

In addition to software attacks against software and physical attacks against hardware-targeted soware attacks, appeared in the mid-2000s software attacks against hardware components. For example the Rowhammer attack aims at flipping memory bits while reading and writing another cell. The insider attacker model moves to an outsider one when using a JavaScript program executed in a browser to perform this attack remotely. Recently it has been shown to be effective when applied on SSD disks (NAND flash technology).

Perturbation can also be generated in multicore SoC using the Dynamic Voltage and Frequency Scaling (DVFS), i.e., the energy management technique that saves energy by regulating the frequency and voltage of the processor cores. It has been shown that a misconfiguration of these two parameters can be used to induce faults in the hardware. Each core being individually controlled, one core can inject a fault in another core. Even if it has not yet been demonstrated, this attack should be achievable from within a browser.

Software-based attacks against hardware make it possible to circumvent security mechanisms implemented at the software level. In fact, the software protections consider that the hardware is working properly, “simply” executing instructions to produce a result. Of course, this is not so easy and errors that can be exploited by attackers can also occur at the hardware level.

More generally speaking, the traditional approach of computer science and technologies, constantly adding new more and more powerful levels of abstraction naturally leads, when proposing a security mechanism at a given level of abstraction, to consider that the lower layers are correct and safe. This is however not the case; this is why the attackers have had a tendency these last years to target less and less abstract layers, successively attacking by software the applications, the OS, their kernel, the firmware, and now the hardware.

These low-layer attacks typically exploit flaws from optimization mechanisms implemented in modern OS’s and processors, such as caches, branch

Phishing

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need – a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with. It's one of the oldest types of cyberattacks, dating back to the 1990s, and it's still one of the most widespread and pernicious, with phishing messages and techniques becoming increasingly sophisticated.

Phish" is pronounced just like it's spelled, which is to say like the word "fish" – the analogy is of an angler throwing a baited hook out there (the phishing email) and hoping you bite. The term arose in the mid-1990s among hackers aiming to trick AOL users into giving up their login information. The "ph" is part of a tradition of whimsical hacker spelling, and was probably influenced by the term "phreaking," short for "phone phreaking," an early form of hacking that involved playing sound tones into telephone handsets to get free phone calls.

Nearly a third of all breaches in the past year involved phishing, according to the 2019 Verizon Data Breach Investigations Report. For cyber-espionage attacks, that number jumps to 78%. The worst phishing news for 2019 is that its perpetrators are getting much, much better at it thanks to well-produced, off-the-shelf tools and templates.

Some phishing scams have succeeded well enough to make waves:

- Perhaps one of the most consequential phishing attacks in history happened in 2016, when hackers managed to get Hillary Clinton campaign chair John Podesta to offer up his Gmail password.
- The "fappening" attack, in which intimate photos of a number of celebrities were made public, was originally thought to be a result of insecurity on

4. These cyberthreats can be generically defined as using computer technology to engage in activity that can undermine a society's ability to maintain internal or external order.

5. You open your email and suddenly an alert from your bank appears in your inbox.

6. Instead of rolling the dice on your password security, consider using a password manager.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. to boot	a) встановлювати
2. app	b) дивитись на сайтах, шукати
3. software	c) додаток
4. to surf	d) взламувати
5. to intercept	e) перехватити (сигнал)
6. to crack	f) шахрайство
7. fraud	g) програмне забезпечення

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. How do phishing attacks work?
2. How do you protect against phishing?
3. Can opening a text be harmful?

prediction, or speculative execution. Indeed, these optimizations create differences in program execution time, thus revealing secret information. For example, the recent Spectre attack exploits branch prediction and speculative execution and exfiltrates information through a covert channel based on cache access. To mitigate this attack, one could refresh the cells (read and re-write their values) periodically. This solution would of course come at the price of performance limitations, as other read operations asked by programs would not be possible during the refreshes. More generally, protection against attacks of this type would involve the limitation, if not the complete elimination, of certain optimizations, of course at the cost of lower performance.

The Rowhammer attack evoked above is a software attack that actually exploits a physical property of matter. Each DRAM cell is composed of a capacitor and a transistor that electrically implement a bit of information. By repeatedly accessing cells, the charge of these cells leaks and electrically interacts with the charge of other neighbor cells. It is thus possible to change the value of a cell (and therefore to violate the integrity of this cell) without having ever accessed it. Here, the protection against the attack should be physical: for example, one could consider limiting the reduction of the component's surface, even if the cost would be of course very important.

Notice that these attacks are not easy to detect as they leave no trace at the operating system or application levels. Finally, it is difficult to know whether attacks of this type have already been used in reality. At the time of this document's writing, it seems much simpler to use much more classical attacks against the software or against users (social engineering).

II. Post-reading activities.

Task 7. Answer the following questions.

1. Can tools consider the interaction of the computing unit with its physical environment?

2. What are the most classic leakages?
3. Does the success depend on the experiment?
4. When do software attacks against software and physical attacks?
5. What are the functions of Software-based attacks?
6. Is each core being individually controlled and can one core inject a fault in another core?
7. What is the Rowhammer attack?
8. Of what is each DRAM cell composed?
9. What are the functions of Java Script?
10. Should the attack be physical?

Task 8. Complete the following sentences using the text.

1. The insider _____ _____moves to an outsider one when using a _____program executed in a browser to perform this attack remotely. Recently it has been shown to be _____when applied on SSD _____ (NAND flash technology).
2. Software-based attacks against hardware make it possible to _____security mechanisms implemented at the software level. In fact, the _____ _____consider that the hardware is working properly, "simply" executing _____to produce a result.
3. These low-layer attacks typically exploit flaws from optimization mechanisms implemented in modern OS's and processors, such as _____, branch prediction, or _____ _____.
4. Indeed, these optimizations create differences in program execution time, thus revealing secret information. For example, the recent _____ _____ exploits branch prediction and speculative execution and exfiltrates information through a covert channel based on _____ access.
5. Of course, this is not so easy and errors that can be exploited by attackers can also occur at the _____level.

Unit 18. Phishing.

I. <u>Pre-reading activities.</u>

Task 1. How do you understand the statement: *"Most hackers are young because young people tend to be adaptable. As long as you remain adaptable, you can always be a good hacker."* – Emmanuel Goldstein.

Translate it into Ukrainian.

Task 2. Discuss the following questions.

1. Why is it called phishing?
2. What is whale phishing?
3. What happens if I open a phishing link?

Task 3. Try to guess the meaning of the following words.

Whale phishing, cyber-attack, CEOs, Trojan horses, attackers, bank phishing, spam, hacking, pop-ups.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. Phishing is the <u>fraudulent use</u> of electronic communications to deceive and take advantage of users.
2. <u>Scammers</u> use email or text messages to trick you into giving them your personal information..
3. Do not click on links or pop-ups, open attachments, or respond to emails from strangers.

Виконання зазначених засобів безпеки дозволить лише мінімізувати можливість випадкового несанкціонованого проникнення у ваші пристрої та системи. Однак неможливо надати повної гарантії уникнення зламу. Для максимальної мінімізації таких ризиків компаніям рекомендовано користуватися послугами спеціалістів у сфері кібербезпеки з чітким виконанням всіх інструкцій, які вони зазначають.

Пам'ятайте, що світ живе в еру інформаційних технологій, коли можливості мережі є не лише приємним джерелом можливостей, знань та спілкування, але й джерелом підвищеної небезпеки бути «відкритою книгою», якщо вами зацікавляться певні особи.

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Зламати систему, соціальна інженерія, хакерські атаки, шахрайство, кіберпростір, кібербезпека, джерело інформації, хакери, шукати в інтернеті, персональні дані, гаджети, платіжні операції, програмне забезпечення, кібератака, вмикати комп'ютер, видаляти програму, операційна система, зареєструватись, друкувати, роздрукувати, додаток, ноутбук, персональний комп'ютер, системний блок, вірус, інформаційні технології, злом, вспливаючі реклами.

6. More generally speaking, the traditional approach of computer science and technologies, constantly adding new more and more _____ _____of abstraction naturally leads, when proposing a security mechanism at a given level of abstraction, to consider that the _____ _____are correct and safe.
7. The Rowhammer attack _____above is a software attack that actually exploits a physical property of matter.
8. Each _____ _____ is composed of a _____and a transistor that electrically implement a bit of information.
9. This solution would of course come at the price of performance _____, as other read operations asked by programs would not be possible during the refreshes.
10. More generally, _____against _____of this type would involve the limitation, if not the complete elimination, of certain _____, of course at the cost of _____performance.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Кібератаки та системи їхнього виявлення

Кібератака (англ. cyber-attack) – спроба реалізації кіберзагрози, тобто будь-яких обставин або подій, що можуть бути причиною порушення політики безпеки інформації і/або завдання збитків автоматизованій системі.

Законодавство України визначає: «Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні,

програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту».

Нижче наведено неповний перелік відомих кібератак (хакерських атак) на автоматизовані та інформаційні системи. Посилання на основні статті про інцидент (там де можливо) виділено жирним шрифтом. [https://uk.wikipedia.org/wiki/Перелік_кібератак]

Система виявлення атак (вторгнень) (англ. Intrusion Detection System, IDS) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет. Про будь-яку активність шкідливого ПЗ або про порушення типової роботи централізовано збирається інформація SIEM-системою (англ. Security information and event management). SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тривог для розрізнення несанкціонованої активності від хибного спрацювання тривоги. Про що оповіщається або адміністратор або операційний центр безпеки.

Деякі системи виявлення вторгнень можуть виявити початок атаки на мережу, причому деякі з них здатні виявляти раніше не відомі атаки. Такі системи називають системами запобігання вторгненням (англ. Intrusion Prevention System, IPS). IPS не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипту, заданого адміністратором). На практиці

метою отримання несанкціонованого доступу до певного ПЗ або системи.

Повністю захистися від кібератак неможливо. Проте виконання хоча б мінімальних правил техніки безпеки поводження в мережі значно підвищить шанси, що вас не зламають. Отже, давайте ознайомимося з основними правилами:

- користуватися виключно офіційним ПЗ і вчасно його оновлювати;
- не завантажувати програмне забезпечення з ненадійних джерел;
- використовувати антивіруси для роботи з комп’ютерами;
- нікому не передавати особисті персональні дані (пін коди карток, CVV коди, паролі до акаунтів тощо), навіть якщо вам намагаються вказати на необхідність таких дій з метою вирішення певного питання;
- створювати складні паролі;
- не здійснювати платіжних операцій у відкритій, незахищеній мережі Wi-Fi;
- намагатися користуватися двофакторною аутентифікацією;
- не відкривати файли та листи від підозрілих джерел;
- не переходити на підозрілі посилання та за спливаючими вікнами;
- не заходити на ненадійні сайти та не завантажувати з них жодних ПЗ;
- не вставляти у свій комп’ютер флешки та зовнішні диски, якщо не довіряєте повністю їх джерелу;
- періодично здійснювати резервне копіювання важливої інформації;
- тримати свої гаджети в полі зору, коли знаходитися у місцях, де до них може бути доступ сторонніх осіб.

підроблений сайт, де необхідно ввести облікові дані. Якщо «жертва» вводить свої дані на таких сайтах, то злочинцям стають відомі ці дані та вони можуть використати їх з метою крадіжки персональних даних, персональних коштів або іншого. Фішинг є одним з найпоширеніших видів кібератак.

2. Вірус – це програма, яка встановлюється без відома та проти волі користувача на його комп'ютер або інший пристрій. Комп'ютерний вірус можна «схопити» по-різному. Наприклад, веб-сторінки та поштові вкладення можуть використовуватися для безпосереднього запуску вірусу в систему. Часто вірус буває вбудований у завантажену з інтернету програму, яка «випускає» вірус на волю, після того як «жертва» її встановлює. Після зараження вірусом програма може заблоковувати доступ до файлів та системи з метою отримання викупу. При цьому сплата викупу не завжди гарантує відновлення роботи системи.

3. Соціальна інженерія – це підхід до злому, який не залежить від технологій і полягає у застосуванні шахраями тактики, завдяки якій вони переконують «жертву» розкрити конфіденційну інформацію. Тактики можуть бути різними: від видавання себе за співробітника банку, знайомого або товариша до різноманітних погроз із вимогою встановити шкідливе ПЗ.

4. Шкідливе ПЗ (Malware) – до таких програм належать так звані «трояни», програми-шпигуни чи рекламне ПЗ. Достатньо часто вони встановлюються разом з іншою, корисною програмою, яку вирішила завантажити «жертва». Такі програми можуть таємно записувати всі натискання на клавіші, сканувати файли на жорсткому диску і читати cookie-файли браузера.

5. Злом – це умисна дія, спрямована на несанкціоноване проникнення у ПЗ або систему шляхом обходу механізму безпеки, з

досить часто програмно-апаратні рішення поєднують у собі функціональність двох типів систем. Їх об'єднання називають IDPS (IDS і IPS).

Хоч існує декілька типів IDS, які за розміром варіюються від окремих комп'ютерів до великих мереж, найпоширенішими класифікаціями є системи виявлення вторгнень у мережу (англ. network intrusion detection systems, NIDS) та системи виявлення вторгнень засновані на аналізі хостів [en] (англ. host-based intrusion detection systems, HIDS). Прикладом HIDS буде система, яка відслідковує важливі файли операційної системи, прикладом NIDS буде система, яка аналізує вхідний мережевий трафік. Також можна класифікувати IDS відповідно до методів виявлення загроз: найбільш відомим є виявлення на основі сигнатур (розпізнавання поганих шаблонів, таких як шкідливе ПЗ) та виявлення аномалій (виявлення відхилень від «правильного» трафіку, часто за допомогою машинного навчання). [https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень]

Task 11. Give the English equivalents of the Ukrainian words and word combinations.

Кіберзагрози, кіберпростір, програмне забезпечення, автоматизовані системи, кіберзахисту, кібератака, SIEM-система, кібероперації, кібернетична безпеки, система виявлення атак, спрямовані (навмисні) дії в кіберпросторі, засоби електронних комунікацій, інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, порушення конфіденційності, доступністі електронних інформаційних ресурсів, шкідливе ПЗ, розрізнення несанкціонованої активності, розрив з'єднання або виконання скрипту, функціональність двох типів систем.

Unit 6. Worms

I. Pre-reading activities.

Task 1. How do you understand the statement: *"What is a Computer Worm"*. **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What is a computer worm?
2. What is the difference between a Computer Worm and a Virus?
3. How does computer worm work?

Task 3. Try to guess the meaning of the following words.

Computer worm, malicious software, malware, operating system, storage media, floppy diskettes

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers.

2. The worm is able to continue to propagate within an organization in this way.

3. Successful email worms usually incorporate social engineering methods to prompt users to open the attached file.

4. A bot worm may be used to infect computers and turn them into zombies or bots, with the intent of using them in coordinated attacks through botnets.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах.

Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

Хакери мають багато можливостей, щоб скористатися вразливістю кібербезпеки та досягти своїх цілей. Сьогодні можна виділити такі основні (найпопулярніші) способи:

1. Фішинг – один з видів інтернет-шахрайства, коли «жертві» надсилаються повідомлення від імені відомих компаній або організацій (наприклад, банку, податкової служби, відомого інтернет-магазину), однак насправді вони не є справжніми. Мета фішингу – отримання доступу до конфіденційних даних користувачів (паролів, логінів, даних особових рахунків і банківських карт). Зазвичай використовується метод проведення масових розсилок від імені популярних компаній або організацій, які містять посилання на фейкові сайти, які важко зовні відрізнити від справжніх. У листах особу ввічливо просять оновити чи підтвердити правильність персональної інформації або інформують про які-небудь проблеми з даними, а після цього перенаправляють на

7. Why is it hard to catch cyber criminals?
8. How can you be cybersmart to stay safe?
9. What is the full form of cyber?
10. Is cybercrime always carried out by a group?

Task 8. Complete the following sentences using the text.

1. Cyberspace is considered "a globally interconnected network of digital information and _____ _____", normally understood to mean the internet and, more broadly, computer networks.
2. The criminal law of _____ is based on actions, such as theft or sexual abuse of a minor
3. In such an approach, commonly seen as authoritarian or anti-liberal, the focus is on the _____
4. However, there is consensus that terrorism is not just _____, but constitutes a special form of crime, characterized by its severity.
5. Similarly, it's not difficult to imagine that, with the rise of terrorism, there has also emerged it's virtual strain: _____.
6. For the same reason, if a single person _____ ___ _____ on a public street there would certainly be some criminal conduct, but not a terrorist act based on the arguments outlined earlier.
7 The _____ of "author" is based on dangerous criminal personality traits, such as if an individual is a thief or pedophile.
8. That _____ is defined by its location or the medium through which it is executed can be criticized to some extent.
9. Much has been written about the _____ of terrorism, but without agreement on its meaning.
10. In relation to these requirements, a doctrine has developed providing _____ to determine whether a "criminal terrorist association" is faced.

5. An ethical worm is a computer worm designed to propagate across networks with the express purpose of delivering patches for known security vulnerabilities.
6. Users should practice good cybersecurity hygiene to protect themselves against being infected with computer worms.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1). duplicates	a). поширювати
2). victim	b). вихідні повідомлення
3). propagate	c). копії
4). outbound	d). кібербезпека
5). payload	e). брандмауери
6). cybersecurity	f). корисне навантаження
7). firewalls	g). жертва

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. How do computer worms spread?
2. How do computer worms work?
3. What are the types of computer worms?

Worms

A computer worm is a type of malicious software program whose primary function is to infect other computers while remaining active on infected systems.

A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers. Worms often use parts of an operating system that are

automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

A computer worm is not to be confused with WORM (write once, read many).

A computer worm infection spreads without user interaction. All that is necessary is for the computer worm to become active on an infected system. Before widespread use of networks, computer worms were spread through infected storage media, such as floppy diskettes, which, when mounted on a system, would infect other storage devices connected to the victim system. USB drives are still a common vector for computer worms.

Computer worms often rely on the actions of, and vulnerabilities in, networking protocols to propagate. For example, the WannaCry ransomware worm exploited a vulnerability in the first version of the Server Message Block (SMBv1) resource sharing protocol implemented in the Windows operating system. Once active on a newly infected computer, the WannaCry malware initiates a network search for new potential victims: systems that respond to SMBv1 requests made by the worm. The worm is able to continue to propagate within an organization in this way. When a bring your own device (BYOD) is infected, the worm can spread to other networks, giving hackers even more access.

Email worms work by creating and sending outbound messages to all the addresses in a user's contacts list. The messages include a malicious executable file that infects the new system when the recipient opens it. Successful email worms usually incorporate social engineering methods to prompt users to open the attached file.

Types of computer worms

There are several types of malicious computer worms:

- A computer virus or worm hybrid is a piece of malware that spreads like a worm, but that also modifies program code like a virus -- or else carries

treats those breaching the rules as enemies of the state rather than citizens "who are simply a source of danger that must be eliminated by any means, whatever the cost" (Cancio Meliá, 2002: 20).

That same form of discussion and analysis is often seen when discussing terrorism, where a (political) opponent is, strategically, labelled a "terrorist" (Mañalich, 2017). In such an approach, commonly seen as authoritarian or anti-liberal, the focus is on the "terrorist." Meanwhile, a liberal approach focuses on the actions of the so called terrorist more than their personal characteristics as a "terrorist."

The final approach to responding to terrorism is the correct one because, amongst other things, not all actions of a "terrorist" or by a member of a terrorist organization can be classified as terrorism or terrorist acts. In reality, a "terrorist" is far more likely to engage in a wide variety of activities ranging from non-criminal (such as spending time with family or driving a car), to committing non-terrorist crimes (such as fraud or drug trafficking), than to actual terrorist attacks (such as bombing the seat of government.)

Джерело: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005

III. Post-reading activities.

Task 7. Answer the following questions.

1. What does cyber mean?
2. What is cyberterrorism?
3. What are cyber terrorism examples?
4. What is the goal of the cyber terrorist?
5. How do you stay safe online?
6. Can cybercrime be stopped?

through which it is carried out: in cyberspace instead of the physical world. From this point of view, cyberterrorism is not an autonomous crime, which should be punished independently. Rather, it implies a kind of terrorism characterized by a unique method of execution.

That cyberterrorism is defined by its location or the medium through which it is executed can be criticized to some extent. To address such criticisms, a comparison can be made to aircraft hijacking terrorist acts, such as the 9/11 terrorist attacks on the World Trade Center; or vehicle-based terrorist attacks, such as when a truck deliberately drove into a crowd of people on the Nice promenade in 2016. In reality, the scope of cyberterrorism appears to follow the general tendency for many "real world" phenomena to be replicated online. Thus, it is common to talk about "cyber activism" (Milan and Hintz, 2013) as a type of activism carried out online; or "cyberbullying" (Kraft and Wang, 2009) being a type of bullying which also occurs online. Similarly, it's not difficult to imagine that, with the rise of terrorism, there has also emerged it's virtual strain: cyberterrorism.

The (cyber)terrorists 'actions and the (cyber)terrorists 'author

The Continental European tradition of criminal law usually differentiates between what an individual does (in other words, their behavior) and who they are (in other words, their character, personal preferences, thoughts, etc.) From this, we can distinguish between the criminal law of "acts" or "facts" (Mir Puig, 2016), consistent with a liberal criminal justice system, and the criminal law of "author" (Velásquez Velásquez, 2009), consistent with an authoritarian criminal justice system. The criminal law of "acts" is based on actions, such as theft or sexual abuse of a minor. The criminal law of "author" is based on dangerous criminal personality traits, such as if an individual is a thief or pedophile. At its core, under the criminal law of "author", a thief or pedophile is marked by a kind of stigma, where independent of their actions, and even though their theft or sexual abuse of minors is now in the past, they will forever be considered a thief or pedophile. This is linked to the concept of criminal law of "the enemy" (Jakobs, 2003), which

some sort of malicious payload, such as a virus, ransomware or some other type of malware.

- A bot worm may be used to infect computers and turn them into zombies or bots, with the intent of using them in coordinated attacks through botnets.
- Instant messaging, or IM worms propagate through instant messaging services and exploit access to contact lists on victim computers.
- Email worms are usually spread as malicious executable files attached to what appear to be ordinary email messages.

Finally, an ethical worm is a computer worm designed to propagate across networks with the express purpose of delivering patches for known security vulnerabilities. While ethical worms have been described and discussed in academia, actual examples in the wild have not been found, most likely because the potential for unexpected harm done to systems that react unexpectedly to such software outweighs the potential for removing vulnerabilities. In any case, unleashing any piece of software that makes changes to a system without the permission of the system owner opens the publisher to various criminal and civil charges.

Differences between worms and viruses

As defined in the "Security of the Internet" report, released in 1996 by the CERT Division of the Software Engineering Institute at Carnegie Mellon University, computer worms "are self-replicating programs that spread with no human intervention after they are started." In contrast, "[v]iruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems."

After a computer worm loads and begins running on a newly infected system, it will typically follow its prime directive: to remain active on an infected system for as long as possible, and to spread to as many other vulnerable systems as possible.

How to prevent a computer worm

Users should practice good cybersecurity hygiene to protect themselves against being infected with computer worms. Measures that will help prevent the threat of computer worm infections include:

- Keeping up to date with operating systems and all other software patches and updates will help reduce the risk due to newly discovered vulnerabilities.
- Using firewalls will help reduce access to systems by malicious software.
- Using antivirus software will help prevent malicious software from running.
- Being careful not to click on attachments or links in email or other messaging applications that may expose systems to malicious software.

Encrypt files to protect sensitive data stored on computers, servers and mobile devices

Although some worms are designed to do nothing more than propagate themselves to new victim systems, most worms are associated with viruses, rootkits or other malicious software.

Джерело: https://searchsecurity.techtarget.com/definition/worm

III. Post-reading activities.

Task 7. Answer the following questions.

1. What types of Computer Worms are there?
2. How do you recognize a Computer Worm?
3. How can one remove a Computer Worm?
4. How can you protect yourself from a Computer Worm?
5. How to prevent a computer worm?
7. How to detect a computer worm?
8. What are the symptoms of a computer worm infection?

Structure

In terms of its structure, terrorism is always organized crime (Cancio Meliá, 2010), as opposed to individual crimes (for example, bodily harm caused by a single person) or crimes carried out by a group on an ad hoc basis (for example, a homicide committed by three individuals: one to subdue the victim, another to stab her in the abdomen, and a third waiting for them in a getaway car.)

In effect, although some authors believe terrorism can be carried out by a single person (Goodman, Kirk and Kirk, 2007), others claim, correctly, that (in practice) there is no such thing as "individual terrorists" acting alone, outside of an organization (Villegas Díaz, 2016). Thus, the specific "danger" implied by terrorism (Cancio Meliá, 2010), which in part justifies its severe punishment in relation to other crimes, lies in the existence of an organized collective that operates systematically to commit an indefinite number of crimes (Gómez Martín, 2010). Regardless of the problematic nature of the concept of "danger", due to its great indeterminacy and incompatibility with the presumption of innocence, such danger does not exist in the case of an individual or ad hoc group acting alone, even if they employ similar methods (for example, explosives) commonly used by terrorist organizations. For the same reason, if a single person detonates a bomb on a public street there would certainly be some criminal conduct, but not a terrorist act based on the arguments outlined earlier.

In relation to these requirements, a doctrine has developed providing criteria to determine whether a "criminal terrorist association" is faced. They are: 1) the existence of a set number of members, 2) access to resources and funding, and 3) a capacity to sustainably plan and carry out operations over time (Mañalich, 2015).

What is cyberterrorism?

Much has also been written on the topic of cyberterrorism, despite lacking a unanimous consensus regarding its scope and meaning. As it were, for cyberterrorism to be, effectively, a form of terrorism, it must meet the structure, harm principle and elements of terrorism. As a result, the scope of cyberterrorism is, as its name suggests, based on the "place" in which it occurs or the "medium"

(Conway, 2014; Denning, 2000). Cyberspace is considered "a globally interconnected network of digital information and communications infrastructures" (Melzer, 2011: 4), normally understood to mean the internet and, more broadly, computer networks (Ambos, 2015; Yannakogeorgos, 2014).

The concept of cyberterrorism usually refers to a range of very different actions, from the simple spread of propaganda online, to the alteration or destruction of information, and even to the planning and carrying out of terrorist attacks via the use of computer networks. As such, in order to better understand what cyberterrorism is, this article will begin by analyzing the concept of "terrorism" –including its structure, harm principle, and elements– as a broad category to which the species "cyberterrorism" belongs; later, it will delimit the idea of cyberterrorism and distinguish it from others with which it has a certain similarity; finally, it will raise some of the most important challenges that cyberterrorism implies in a global and technologically interconnected world.

What is terrorism?

Much has been written about the concept of terrorism, but without agreement on its meaning. Many authors on this topic have pointed out the difficulties in forming a legal definition of terrorism, differentiating it from other types of crimes (Fletcher, 2006; Guzmán Dalbora, 2017). However, there is consensus that terrorism is not just regular crime, but constitutes a special form of crime, characterized by its severity (Teixeira, 2013). In that sense, "the better way to think of terrorism . . . is not as a crime but as a different dimension of crime, a higher, more dangerous version of crime, a kind of super-crime incorporating some of the characteristics of warfare" (Fletcher, 2006: 900).

In considering some of the main ideas developed in relation to the legal definition of terrorism in the Continental European framework, there is general agreement in how it relates to the structure, harm principle and elements of terrorism. The Continental European framework is relevant because of its extensive work on the theoretical-dogmatic concept of terrorism.

10. What is history of computer worms?
11. Which computer worms do you know?

Task 8. Complete the following sentences using the text.

1. It is common for worms to be noticed only when their uncontrolled _____ consumes system resources, slowing or halting other tasks.

2. USB drives are still a common _____ for computer worms.

3. Computer worms often rely on the actions of, and _____ in, networking protocols to propagate.

4. Email worms work by creating and sending _____ messages to all the addresses in a user's contacts list.

5. Successful email worms usually _____ social engineering methods to prompt users to open the attached file.

6. Email worms are usually spread as malicious _____ files attached to what appear to be ordinary email messages.

7. In any case, unleashing any piece of _____ that makes changes to a system without the permission of the system owner opens the publisher to various criminal and civil charges.

8. Using firewalls will help reduce access to systems by _____ software.

9. _____ files to protect sensitive data stored on computers, servers and mobile devices

10. The worm is able to continue to _____ within an organization in this way.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Хробак комп'ютерний – це програма, яка може подолати всі три етапи розповсюдження самостійно (звичайний хробак), або використовує агента-користувача тільки на 2-му етапі (поштовий черв'як). Хробаки майже завжди шкодять мережі, наприклад, споживаючи пропускну здатність. Більшість створених комп'ютерних хробаків лише розповсюджуються, та не шкодять системам.

Одні з перших експериментів по використанню комп'ютерних хробаків в розподілених обчисленнях відбулися в дослідницькому центрі Xerox в Пало-Альто Джоном Шочем та Йоном Хуппом в 1978. Термін виник під впливом науково-фантастичних романів Девіда Герролда «Коли ХАРЛІ виповнився рік» та Джона Браннера «На ударній хвилі»

Одним з найвідоміших комп'ютерних хробаків є «Хробак Моріса», написаний Робертом Морісом-молодшим, який був в той час студентом Корнельского Університету. Поширення хробака почалось 2 листопада 1988, після чого хробак швидко заразив велику кількість комп'ютерів, під'єднаних до інтернету.

Хробаки можуть використовувати різноманітні механізми («вектори») поширення. Деякі хробаки потребують певних дій користувача для поширення (наприклад, відкриття інфікованого повідомлення в клієнті електронної пошти). Інші хробаки можуть поширюватися автономно, вибираючи та атакуючи комп'ютери в повністю автоматичному режимі. Іноді зустрічаються хробаки з цілим набором різноманітних векторів поширення, стратегій вибору жертви, і навіть експлойтів під різні операційні системи.

Хробаки можуть складатися з різних частин. Часто виділяють так звані резидентні хробаки, які можуть інфікувати працюючу програму і знаходиться в оперативній пам'яті комп'ютера, при цьому не зачіпаючи тверді диски. Від подібних хробаків можна позбутися перезапуском комп'ютера (і, відповідно, очищенням оперативної пам'яті). Ці хробаки

6 At the same time, the prototypical term "electronic Pearl Harbor" was coined, linking the threat of a computer attack to an American historical trauma.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. fraud	a) взламувати
2. VPN	b) дискета
3. software	c) віртуальна приватна мережа
4. floppy disc	d) друкувати
5. to browse	e) шукати
6. to crack	f) шахрайство
7. to type	g) програмне забезпечення

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. Why is cyberterrorism so dangerous for our society?
2. What is cyberterrorism?
3. What are the criteria to determine whether a "criminal terrorist association" is faced?

Cyber terrorism

The term "cyberterrorism" is complex and combines two concepts: "cyber", referring to cyberspace, and "terrorism", whose meaning and scope will be analyzed later. On this basis, we can assume that cyberterrorism is a special type of terrorism, where the "place" or "medium" it is carried out in is cyberspace

Unit 17. Cyber terrorism

I. Pre-reading activities.

Task 1. How do you understand the statement: *"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it."* – (Stephane Nappo). **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What do you understand under the term ciber terrorism?
2. What is the goal of the cyber terrorist?
3. What's another word for cyber?

Task 3. Try to guess the meaning of the following words.

cyber, organized crime, victim, vehicle-based terrorist attacks, fraud, ad hoc group, cyber activism, hacking, cyber weapons.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. Do not click on links or pop-ups, open attachments, or respond to emails from strangers.

2. Choose a password that means something to you and you only and change your passwords on a regular basis.

3. If you see something suspicious, report it to the proper authorities.

4. These cyberthreats can be generically defined as using computer technology to engage in activity that can undermine a society's ability to maintain internal or external order.

5. India has the maximum internet users, called as 'Netizens' after USA and China.

складаються в основному з «інфекційної» частини: експлойта (шелл-кода) і невеликого корисного навантаження (самого тіла хробака), яке міститься повністю у пам'яті. Специфіка подібних хробаків полягає в тому, що вони не завантажуються через завантажувач як всі звичайні виконувані файли, тому відповідно, можуть розраховувати лише на ті динамічні бібліотеки, які вже були завантажені в пам'ять іншими програмами. Також існують хробаки, які після вдалого інфікування пам'яті зберігають код на твердому диску й вживають заходів для наступного запуску цього коду (наприклад, прописують відповідні ключі в реєстрі Windows). Від таких хробаків можна позбутися лише за допомогою антивіруса або подібних інструментів. Часто інфекційна частина таких хробаків (експлойт, шелл-код) містить невелике корисне навантаження, яке завантажується в оперативну пам'ять і може «довантажити» через мережу саме тіло хробака в вигляді окремого файла. Для цього деякі хробаки можуть містити в інфекційній частині простий TFTP-клієнт. Завантажене таким способом тіло хробака (зазвичай окремий виконуваний файл) тепер відповідає за подальше сканування та поширення вже з інфікованої системи, а також може містити серйозніше, повноцінне корисне навантаження, ціллю якого може бути, наприклад, нанесення певної шкоди (наприклад, DoS-атаки).

Більшість поштових хробаків поширюються як один файл. Їм не потрібна окрема «інфекційна» частина, так як зазвичай користувач-жертва за допомогою поштового клієнта добровільно завантажує та запускає хробака.

Часто хробаки навіть без певного корисного навантаження завантажують і тимчасово виводять з ладу мережі лише за рахунок інтенсивного поширення.

Якщо код комп'ютерного хробака призначений на більше, ніж просте поширення хробака його називають хробаком «корисного навантаження». Типові хробаки корисного навантаження можуть видаляти файли на хост-системі, шифрувати файли для отримання грошового викупу або копіювати дані, такі як паролі або конфіденційні документи. Найбільш поширене

корисне навантаження для хробаків є встановлення у систему, так званих, бекдорів. Це дозволяє зловмиснику віддалено контролювати комп'ютером, створюючи «зомбі комп'ютер». Мережі, які складаються з таких підконтрольних машин часто називають ботнетами. Такі мережі використовуються для ряду шкідливих цілей, наприклад, для розсилки спаму або для виконання DoS-атаки.

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Зловмисне програмне забезпечення, шкідливе програмне забезпечення, копія, сховище інформації, дискети, кібербезпека, потенційна жертва, програма-вимагач, ботнети, доступ, програмне забезпечення, цивільні звинувачення, програми, що самовідтворюються, брандмаузер, антивірусне програмне забезпечення, шифровані файли.

• відмова сервісу– атаки з великої кількості комп’ютерів, основною метою яких є порушення функціонування сайтів або комп’ютерних систем;

• втручання в роботу обладнання – атаки, що зазвичай спрямовані на комп’ютери або сервери, які забезпечують роботу систем обробки чи передачі інформації;

• атаки на об’єкти критичної інфраструктури – атаки на комп’ютери та системи, що забезпечують життєдіяльність міст, наприклад: системи водопостачання, електроенергії, транспорту тощо.

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Хакер, комп’ютерні вандали, соціальна інженерія, хакерські атаки, шахрайство, кіберпростір, кібер атака, джерело інформації, зламати сайт, шукати в інтернеті, вкрасти персональні дані, шкідливе влкадення, кібератака, кібер-злочинець, видаляти програму, надійні паролі, зареєструватись, скачати антивірус, нелегальний, додаток, персональний комп’ютер, вірус, інформаційні технології, злом, вспливаючі реклами, Троянський кінь, підозрілі джерела.

телекомунікації та глобальні комп'ютерні мережі, слід знати й розуміти, які можливості для зловживання створюють ці технології. Сьогодні жертвами хакерів можуть стати не лише люди, але й держави в цілому. За ефективністю та наслідками застосування «кіберзброї», а саме такий термін все частіше використовують вчені, можна прирівняти до зброї масового ураження.

Кібербезпека – одна з основних проблем, що викликає занепокоєння. Чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем. Оскільки критичні вразливості в програмному забезпеченні та автоматизованих системах викликають небезпідставні побоювання, то не дивно, що суспільство в усьому світі шукає кращих заходів і методів для захисту особистих даних Інтернет-ресурсів від кіберзагроз.

На перший погляд може здатися, що кібератаки не можуть завдати великої шкоди, але це лише на перший погляд. Розглянемо більш детально, до яких наслідків може призвести кожна з кібератак, що використовуються під час проведення кібероперацій:

• вандалізм – атака, яка, зазвичай не несе матеріальної шкоди, але завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат. До таких кібернетичних атак можна віднести псування офіційних Інтернет-сторінок, заміну змісту образливими чи пропагандистськими малюнками, тощо;

• пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення;

• збір інформації – злам приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні. У цьому випадку дезінформація та викрадення даних. Інша назва – кібершпигунство;

Unit 7. Trojan horse

I. <u>Pre-reading activities.</u>

Task 1. How do you understand the statement: *"I think computer viruses should count as life"*. **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. Which computer viruses do you know?
2. What do you think about computer viruses?
3. Is virus dangerous?

Task 3. Try to guess the meaning of the following words.

Malware, legitimate software, cyber-thieves, sensitive data, harmless programs, various threats..

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. Trojans can be employed by cyber-thieves and hackers trying <u>to gain</u> access to users' systems.
2. You will sometimes hear people refer to a "Trojan virus" or a "Trojan horse virus," but these terms are slightly <u>misleading.</u>
3. It is more useful to think of "Trojan" as an umbrella term for malware delivery, which hackers use for <u>various threats</u>.
4. This is known as "<u>scareware</u>". In reality, users are downloading a Trojan onto their device.
5. When the user connects to this network, they can be redirected to fake websites containing browser exploits that <u>redirect</u> any file they try to download.

6. Usually, they are implemented as scripts or small applications.

7. Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.

8. If you suspect your device may have been breached by Trojan malware, you should look out for the following signs.

9. Poor device performance – for example, running slowly or frequently crashing.

10. Attackers install a Trojan through exploiting a software vulnerability or through unauthorized access.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. misleading	a) помилкове програмне забезпечення
2. scareware	b) додаток
3. rebooting	c) спливаюче вікно
4. backdoor	d) перезавантаження
5. application	e) система електронних платежів
6. e-payment systems	f) таємний
7. pop-up	g) вводити в оману

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What do you know about Trojan Horse?
2. Is it a virus or is it malware?
3. How do Trojans work?
4.

3. There are _____ _____that devote time and effort to acts of computer vandalism that can damage your computers and data, and affect the services that businesses deliver.

4. The programmer's objective is to research the potential of _____ _____.

5. So, the Internet has made it much easier for the _____ to create their own viruses.

6. In many cases, students – that have just understood the use of a _____ _____ – may want to try out their skills, test their ability or prove how clever they are.

7. Today, there are still four main types _____ _____.

8. With widespread _____ _____, these arrests have probably deterred many youths from developing malicious code.

9. In ___ _____, it was a lot easier to create computer viruses that targeted Microsoft's DOS operating system – when compared with the effort required to target today's more complex Windows operating system.

10. Unfortunately, the same type of behavior is also present in _____.

Task 10. Translate from Ukrainian into English.

Вандалізм – використання хакерами інтернету для паплюження інтернет сторінок, заміни змісту образливими чи пропагандистськими зображеннями.

Подібна діяльність поширюється і на приватних осіб, і на громадську власність. Комп'ютерний вандалізм – цу нанесення шкоди комп'ютерній системі або обладнанню без отримання вигоди. Вік цього явища як обчислюється тисячоліттями. Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Сьогодні ми все більше й більше використовуємо їх у своїй діяльності. Але використовуючи

- Linux computers
- Apple Macs
- Smartphones
- Tablets

Джерело: https://www.kaspersky.com/resource-center/threats/computer-vandalism

III. Post-reading activities.

Task 7. Answer the following questions.

1. What is meant by hacker?
2. What is meant by cyber crime?
3. What's another word for cyber?
4. What is anti-malware software?
5. What do you think are the reasons for vandalism?
6. Is cyber vandalism a crime?
7. What does a hacker do?
8. What brand has anti-malware solutions?
9. Name four main types of computer vandal.
10. Why are malicious programs dangerous for us?

Task 8. Complete the following sentences using the text.

1. Today, many computer-literate youths are more likely to become gamers – rather than _____ _____.
2. Older, talented programmers can create very ‘professional ’computer _____.

Trojan Horse

Trojan definition

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

What is a Trojan?

The term “Trojan” derives from the ancient Greek story about the deceptive Trojan horse which led to the fall of the city of Troy. When it comes to your computer, a Trojan virus operates similarly – it hides within seemingly harmless programs or tries to trick you into downloading it. The name was coined in a US Air Force report in 1974, which speculated on hypothetical ways computers could be compromised.

You will sometimes hear people refer to a "Trojan virus" or a "Trojan horse virus," but these terms are slightly misleading. This is because, unlike viruses, Trojans don’t self-replicate. Instead, a Trojan horse spreads by pretending to be useful software or content while secretly containing malicious instructions. It is more useful to think of “Trojan” as an umbrella term for malware delivery, which hackers use for various threats.

How do Trojans work?

A Trojan must be executed by its victim to do its work. Trojan malware can infect devices in several ways – for example: A user falls victim to a phishing or other social engineering attack by opening an infected email attachment or clicking on a link to a malicious website.

A user sees a pop-up for a fake antivirus program that claims your computer is infected and invites you to run a program to clean it up. This is known as “scareware”. In reality, users are downloading a Trojan onto their device.

A user visits a malicious website and experiences a drive-by download pretending to be helpful software.

A user downloads a program whose publisher is unknown from an untrustworthy website.

Attackers install a Trojan through exploiting a software vulnerability or through unauthorized access.

Hackers create a fake Wi-Fi hotspot network that looks like one a user is trying to connect to. When the user connects to this network, they can be redirected to fake websites containing browser exploits that redirect any file they try to download.

The term “Trojan dropper” is sometimes used in relation to Trojans. Droppers and downloaders are helper programs for various types of malware, including Trojans. Usually, they are implemented as scripts or small applications. They don’t carry any malicious activity themselves but instead pave the way for attacks by downloading, decompressing, and installing the core malicious modules.

Types of Trojans

Trojans are classified according to the type of actions that they can perform on your computer. Trojan horse virus examples include:

Backdoor

A backdoor Trojan gives malicious users remote control over the infected computer. They enable the author to do anything they wish on the infected computer – including sending, receiving, launching, and deleting files, displaying data, and rebooting the computer. Backdoor Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.

Exploit

Exploits are programs that contain data or code that takes advantage of a vulnerability within application software that's running on your computer.

Banker Trojan

software. The programmer’s objective is to research the potential of ‘computer fauna’. The programmer may choose not to spread their creations – but actively promote their ideas, via numerous Internet resources that are devoted to the creation of computer viruses. Those ideas and ‘research viruses ’may then be used by malicious individuals or criminals.

Today’s vandalism computer threats

Although all of these groups are still developing computer viruses, there has been a reduction in the number of new, ‘traditional ’types of computer threats that are being released. There are several possible reasons why:

- *New laws*

In many countries, changes in legislation have resulted in the arrest of computer virus writers. With widespread press coverage, these arrests have probably deterred many youths from developing malicious code.

- *Games*

Network games have offered another way for young people to show their skills and prowess. Today, many computer-literate youths are more likely to become gamers – rather than malware creators.

- *Complexity*

In the 1990s, it was a lot easier to create computer viruses that targeted Microsoft’s DOS operating system – when compared with the effort required to target today’s more complex Windows operating system.

While the fall in computer vandalism is to be welcomed, the risks presented by other types of malicious programs represent a much more dangerous threat to your computer… your data… your digital identity… and your finances.

How to protect yourself against Computer Vandalism

Anti-malware software is vital in defending your computer, mobile devices and data against computer vandalism, viruses, worms, Trojans and other malware. Kaspersky Lab has anti-malware solutions that deliver world-class protection for a wide range of computers and other devices, including:

- Windows PCs

computer vandalism that can damage your computers and data, and affect the services that businesses deliver.

Who are the computer vandals?

In the early days of the development of malware, the majority of computer viruses and Trojans were created by students and other young programmers – plus some older, more experienced programmers. Today, there are still four main types of computer vandal:

- *Skilled students… showing off!*

In many cases, students – that have just understood the use of a programming language – may want to try out their skills, test their ability or prove how clever they are. Fortunately, many of these malware creators do not actually distribute their malware – instead, they may send the virus or worm virus to an antivirus company.

- *Inexperienced youths… assisted by the Internet*

Young people that haven't quite understood the art of programming may also turn to computer vandalism – sometimes to prove their 'self-worth'. In the past, this resulted in primitive viruses. However, there are now numerous websites that explain how to write and distribute computer viruses – and how viruses can sidestep antivirus software. So, the Internet has made it much easier for the inexperienced to create their own viruses.

- *Professional developers'*

As young virus writers mature, their experience can make their activities much more dangerous. Older, talented programmers can create very 'professional ' computer viruses. These can be sophisticated programs that use innovative methods to intrude into data system domains, or can exploit security vulnerabilities within operating environments, capitalize on social engineering or use a range of other tricks.

- *Researchers*

These are shrewd programmers that are capable of inventing new methods of infecting computers, concealing the infection and resisting the actions of antivirus

Trojan-Banker programs are designed to steal your account data for online banking systems, e-payment systems, and credit or debit cards.

Clampi Trojan

Clampi – also known as Ligats and Ilomo – lies in wait for users to sign in to make a financial transaction, such as accessing online banking or entering credit card information for an online purchase. Clampi is sophisticated enough to hide behind firewalls and go undetected for long periods.

Cryxos Trojan

Cryxos is commonly associated with so-called scareware or fake support call requests. Typically, victims receive a pop-up containing a message like "Your device has been hacked" or "Your computer is infected". The user is directed to a phone number for support. If the user calls the number, they are pressured to pay for assistance. In some cases, the user may be asked to give remote access of their machine to the "customer service agent", potentially leading to device hijack and data theft.

DDoS Trojan

These programs conduct DDoS (Distributed Denial of Service) attacks against a targeted web address. By sending multiple requests – from your computer and several other infected computers – the attack can overwhelm the target address, leading to a denial of service.

Downloader Trojan

Trojan-Downloaders can download and install new versions of malicious programs onto your computer – including Trojans and adware.

Dropper Trojan

These programs are used by hackers to install Trojans or viruses – or to prevent the detection of malicious programs. Not all antivirus programs are capable of scanning all of the components inside this type of Trojan.

FakeAV Trojan

Trojan-FakeAV programs simulate the activity of antivirus software. They are designed to extort money from you – in return for the detection and removal of threats, even though the threats they report are non-existent.

How Trojans can impact you.

Trojans are incredibly good at hiding. They trick users into installing them and then work behind the scenes to achieve their aim. If you fall victim, you may not even realize it until it's too late. If you suspect your device may have been breached by Trojan malware, you should look out for the following signs:

Poor device performance – for example, running slowly or frequently crashing (including the infamous “blue screen of death”).

The desktop has changed – for example, the screen resolution has altered, or the color appears different.

The taskbar has changed – or perhaps disappeared altogether

Unrecognized programs appear in your task manager – you didn’t install them

An increase in pop-ups – not just ads but browser pop-ups offering products or antivirus scans which, when clicked on, download malware onto your device.

Being redirected to unfamiliar websites when browsing online

An uptick in spam emails

It is possible to remove some Trojans by disabling start-up items on your computer which don’t come from trusted sources. To this, reboot your device into safe mode so that the Trojan can’t stop you from removing it.

Be clear about which specific programs you are removing because you could slow or disable your system if you remove basic programs your computer needs to function.

Джрело: https HYPERLINK "https://www.kaspersky.com/resource-center/threats/trojans" HYPERLINK "https://www.kaspersky.com/resource-center/threats/trojans" HYPERLINK "https://www.kaspersky.com/resource-center/threats/trojans"

5. People, not computers, create computer security threats and malware.

6. Antivirus solutions with identity theft protection can be "taught" to recognize the threat in fractions of a second.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. to hack	a) виявити
2. to detect	b) запит
3. back-up copy	c) резервна копія
4. to erase	d) взламувати
5. to intercept	e) перехватити (сигнал)
6. query	f) шахрайство
7. fraud	g) видаляти

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What is a computer vandalism?
2. Who are cyber vandals?
3. How can I protect my computer from cyber vandalism?

Computer vandalism

In everyday life, there are vandals that seem to enjoy destroying things – even though it can be hard to understand how they derive any tangible benefit from their acts of vandalism. Unfortunately, the same type of behavior is also present in cyberspace. There are malware creators that devote time and effort to acts of

Unit 16. Computer vandalism

I. Pre-reading activities.

Task 1. How do you understand the statement: *"Hacking is not a crime, it's a profession till the time you play with it safely."* - Blank Lined Journal With Calendar For Techies.

Translate it into Ukrainian.

Task 2. Discuss the following questions.

1. What are the dangers of computer vandalism?
2. How can cyber-crimes be safe?
3. Why is it hard to catch cyber criminals?

Task 3. Try to guess the meaning of the following words.

vandalism, cyber-attack, cyberspace, Trojan horses, attackers, virus, worms, hacking, cyber threats.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. Harassment through e-mails is not a new concept
2. Scammers use email or text messages to trick you into giving them your personal information.
3. Intellectual property consists of a bundle of rights.
4. These cyberthreats can be generically defined as using computer technology to engage in activity that can undermine a society's ability to maintain internal or external order.

Task 7. Answer the following questions.

1. Give the definition of a Trojan horse?
2. Name common types of Trojan malware, from A to Z
3. What examples of Trojan malware attacks do you know?
4. How Trojans impact mobile devices?
5. How to help protect against Trojans?
6. Is Trojan virus dangerous?
7. Can Trojan virus be removed?
8. How do you know if you have a Trojan virus?
9. What is the best Trojan remover?
10. Who created Trojan virus?

Task 8. Complete the following sentences using the text.

1. The term "Trojan dropper" is sometimes used in _____ to Trojans.
2. A Trojan horse or Trojan is a type of _____ that is often disguised as legitimate software.
3. It is more useful to think of "Trojan" as an umbrella term for malware delivery, which _____ use for various threats.
4. A user falls victim to a phishing or other social engineering attack by opening an infected email _____ or clicking on a link to a malicious website.
5. Trojans are classified _____ the type of actions that they can perform on your computer.
6. _____ are programs that contain data or code that takes advantage of a vulnerability within application software that's running on your computer.
7. These programs are used by hackers _____ Trojans or viruses – or to prevent the detection of malicious programs.
8. . If you fall victim, you may not even _____ it until it's too late.

9. Be clear about which specific programs you are _____ because you could slow or disable your system if you remove basic programs your computer needs to function.

10. They are designed to extort money from you – in return for the _____ and removal of threats, even though the threats they report are non-existent.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Найкращим поясненням різниці між троянським програмним забезпеченням та вірусом чи зловмисним програмним забезпеченням є історія про Троянську війну та троянську коня.

Що таке троянський кінь? У ході розповіді, греки побудували величезного дерев'яного коня, наповненого солдатами, і подарували коня як дарувальний подарунок місту Трої. Як тільки кінь опинився всередині міста, грецькі солдати виповзли з порожнього коня і напали на місто під покровом темряви.

Віруси - це програмне забезпечення, яке створюється для зараження одного комп'ютера, а потім поширюється на інші комп'ютери. Троянське програмне забезпечення не створене для поширення. Це призначено для виконання дуже конкретного завдання на вашому комп'ютері чи мобільному пристрої.

Троянський вірус призначений для виконання шкідливих завдань на вашому комп'ютері, як правило, навіть не знаючи про це.

Ці завдання можуть:

- Перехоплювати свій інтернет-трафік, щоб викрасти інформацію про банківський рахунок або кредитну карту.

Далі наведено фрагмент псевдокоду на стороні сервера, який використовується для відображення останнього коментаря на веб-сторінці:

надрукувати "<html>"
надрукувати "<h1> Останній коментар </h1>"
надрукувати database.latestComment
надрукувати "</html>"

Наведений вище скрипт просто бере останній коментар з бази даних і включає його в HTML-сторінку. Передбачається, що роздрукований коментар складається лише з тексту і не містить тегів HTML або іншого коду. Він вразливий до XSS, оскільки зловмисник може надіслати коментар, що містить зловмисне корисне навантаження, наприклад:

<script> doSomethingEvil (); </script>

Веб-сервер надає такий HTML-код для користувачів, які відвідують цю веб-сторінку:

<html>
<h1> Останній коментар </h1>
<script> doSomethingEvil (); </script>
</html>

Коли сторінка завантажується в браузері жертви, виконується скрипт зловмисника. Найчастіше жертва цього не усвідомлює і не в змозі запобігти такому нападу.

• JavaScript у сучасних браузерах може використовувати API HTML5. Наприклад, він може отримати доступ до геолокації користувача, веб-камери, мікрофона та навіть певних файлів із файлової системи користувача. Для більшості цих API потрібна можливість користувача, але зловмисник може використовувати соціальну інженерію, щоб обійти це обмеження.

Вищевказане, у поєднанні з соціальною інженерією, дозволяють злочинцям здійснювати розширені атаки, включаючи крадіжку cookie, підсаджування троянів, кейлоггінг, фішинг та крадіжку особистих даних. Вразливості XSS є ідеальним підґрунтям для ескалації атак на більш серйозні. Міжсайтовий сценарій також може використовуватися разом з іншими типами атак, наприклад, підробкою запитів між сайтами (CSRF).

Існує кілька типів атак міжсайтових скриптів: збережений / постійний XSS, відображений / непостійний XSS та XSS на основі DOM. Детальніше про них ви можете прочитати у статті під назвою Типи XSS.

Типова атака XSS має два етапи:

1. Щоб запустити зловмисний код JavaScript у браузері жертви, зловмисник повинен спочатку знайти спосіб ввести шкідливий код (корисне навантаження) на веб-сторінку, яку відвідує жертва.

2. Після цього жертва повинна відвідати веб-сторінку зі шкідливим кодом. Якщо атака спрямована на конкретних жертв, зловмисник може використовувати соціальну інженерію та / або фішинг, щоб надіслати зловмисну URL-адресу жертві.

Щоб перший крок став можливим, вразливий веб-сайт повинен безпосередньо включати введення користувача на своїх сторінках. Потім зловмисник може вставити шкідливий рядок, який буде використовуватися на веб-сторінці та оброблятися браузером жертви як вихідний код. Існують також варіанти XSS-атак, коли зловмисник заманює користувача на відвідування URL-адреси за допомогою соціальної інженерії, а корисне навантаження є частиною посилання, яке користувач натискає.

- Приєднувати свій комп’ютер до більшого «ботнету» в Інтернеті, щоб виконувати злочинні дії, такі як напади відмови в обслуговуванні (DDoS).
- Пошкоджувати свої системні файли і зробіть ваш комп'ютер невідповідним, щоб хакер міг вимагати від вас гроші.
- Збирання електронних адрес або номерів телефонів, які хакери потім продають спамерам.

Троянці можуть бути дуже дорогими. Одним з найвідоміших троян був вірус ФБР MoneyPak, який змусив комп’ютери користувачів не реагувати і порадив користувачам надсилати від $ 200 до $ 400 для відновлення системи. На жаль, багато людей заплатили хакерам.

На жаль, отримати троянський вірус так само просто, як завантажити неправильну програму на комп’ютер або мобільний пристрій. І навіть якщо ви ніколи не завантажуєте програмне забезпечення, все одно можливо ненавмисно перенести одне із цих шкідливих програм на свій комп’ютер.

Віруси та зловмисне програмне забезпечення можуть дратувати, але деякі речі є такими ж шкідливими, як і троянський вірус. Коли ваш комп'ютер заразиться одним із них, його неможливо неможливо видалити. Найкращий захист – це взагалі не уникати зараження.

Встановіть якісне антивірусне програмне забезпечення. Увімкніть автоматичні оновлення Windows, щоб ваша ОС завжди була виправлена. Використовуйте сервіси електронної пошти, які автоматично сканують додатки на віруси, як-от функція сканування вкладень Gmail. Ніколи не натискайте посилання електронної пошти та не перевіряйте підозрілі посилання, перш ніж натискати на них. Уникайте відвідування веб-сайтів, створених лише для розміщення безкоштовного програмного забезпечення.

Ніколи не завантажуйте файли з темної мережі. Використовуйте доповнення до веб-переглядача, що блокує рекламу, і в білий список лише відомих безпечних веб-сайтів.

Ваша найкраща захист – це гарне резервне копіювання Навіть найбільш обережні користувачі можуть опинитися зараженими трояном. Найкращий

спосіб захистити себе - ніколи не залишати себе повністю залежним від файлів, що зберігаються на вашому комп’ютері. Використовуйте програмне забезпечення для резервного копіювання для повного резервного копіювання комп'ютерної системи. Принаймні, обов'язково зберігайте важливі файли лише на зовнішніх жорстких дисках, а ті диски відключаються від комп'ютера, коли файли вам не потрібні.

Якщо повністю створити резервну копію системи, якщо троянин коли-небудь захопить вашу систему і хакери намагаються використати вас за гроші, ви можете виконати повне відновлення системи і назавжди позбутися цих хакерів.

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Компю’терний вірус, шкідливе програмне забезпечення, законне програмне забезпечення, кібер-злодії, конфіденційні дані, нешкідлива програма, спливаюче вікно, корисне програмне забезпечення, ненадійний веб-сайт, несанкціонований доступ, точка доступу, завантаження, ядро шкідливих модулів, пульт, запуск, зомбовані мережі, додаток, особисті дані, фінансова операція, фальсифікований, брандмауери, викрадення пристрою.

Якщо зловмисник може зловживати вразливістю XSS на веб-сторінці для виконання довільного JavaScript у веб-переглядачі користувача, безпека цього вразливого веб-сайту або вразливої веб-програми та його користувачів порушена. XSS не є проблемою користувача, як будь-яка інша уразливість системи безпеки. Якщо це впливає на ваших користувачів, воно впливає і на вас.

Міжсайтові скрипти також можуть використовуватися для викривлення веб-сайту замість націлювання на користувача. Зловмисник може використовувати введені скрипти, щоб змінити вміст веб-сайту або навіть перенаправити браузер на іншу веб-сторінку, наприклад, ту, яка містить шкідливий код.

Що може зробити атакуючий з JavaScript?

Вразливості XSS сприймаються як менш небезпечні, ніж, наприклад, вразливості SQL Injection. Наслідки можливості запуску JavaScript на веб-сторінці спочатку можуть здатися не страшними. Більшість веб-браузерів використовують JavaScript у дуже жорстко контрольованому середовищі. JavaScript має обмежений доступ до операційної системи та файлів користувача. Однак JavaScript все ще може бути небезпечним, якщо його неправильно використовувати як частину шкідливого вмісту:

• Шкідливий JavaScript має доступ до всіх об’єктів, до яких має доступ решта веб-сторінки. Сюди входить доступ до файлів cookie користувача. Файли cookie часто використовуються для зберігання токенів сеансів. Якщо зловмисник може отримати сеансовий файл cookie користувача, він може видавати себе за користувача, виконувати дії від імені користувача та отримувати доступ до конфіденційних даних користувача.

• JavaScript може читати DOM браузера та вносити в нього довільні зміни. На щастя, це можливо лише на тій сторінці, де працює JavaScript.

• JavaScript може використовувати об'єкт XMLHttpRequest для надсилання HTTP-запитів із довільним вмістом у довільні цільові адреси.

9. If the attack is _____ at particular victims, the attacker can use social engineering and/or phishing to send a malicious URL to the victim.

10. The above, in combination with social engineering, allow criminals to pull off advanced attacks including cookie theft, planting trojans, _____, phishing, and identity theft.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Міжсайтове скриптування

Міжсайтовий скрипт (XSS) – це атака введення коду на стороні клієнта. Зловмисник прагне виконати шкідливі скрипти у веб-браузері жертви, включивши шкідливий код у законну веб-сторінку або веб-програму. Фактична атака відбувається, коли жертва відвідує веб-сторінку або веб-програму, яка виконує зловмисний код. Веб-сторінка або веб-програма стає засобом доставки шкідливого скрипту до браузера користувача. Вразливі транспортні засоби, які зазвичай використовуються для атак міжсайтових сценаріїв, – це форуми, дошки оголошень та веб-сторінки, що дозволяють коментувати.

Веб-сторінка або веб-програма є вразливою до XSS, якщо вона використовує несаніфіковані введені користувачем вхідні дані, які генерує. Потім цей ввід користувача повинен проаналізувати браузер жертви. Атаки XSS можливі у VBScript, ActiveX, Flash і навіть CSS. Однак вони найчастіше зустрічаються в JavaScript, насамперед тому, що JavaScript є фундаментальним для більшості переглядів веб-сторінок.

"Хіба міжсайтовий скрипт не має проблеми з користувачами?"

Unit 8. Scareware

I. <u>Pre-reading activities</u>

Task 1. How do you understand the term "Shareware"

Task 2. Discuss the following questions

1. What is meant by shareware?
2. Does shareware still exist?
3. Is shareware legal?

Task 3. Try to guess the meaning of the following words.

Pop-up windows, antimalware program, antivirus program, restart , trick, remotely.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. The first one is <u>identity theft</u> – the scareware program will install a malicious key logger program to your device to record everything you type.
2. Open your antivirus software and <u>run</u> a full scan to determine if there are any viruses present on your computer.
3. Lastly, the third goal of scareware programs is to turn your computer into a "<u>zombie"</u>

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. firewall	a) доступ
2. button	b) шахрайство
3. access	c) завантажити
4. scam	d) мережевий екран
5. wireless	e) безпровідний
6. download	f) встановити
7. install	g) кнопка

II. <u>While-reading activities.</u>

Task 6. Read the text and answer the questions. Translate the text into Ukrainian

1. When did this program first appear?
2. Why do hackers use scareware?
3. How can you protect your personal data during a scareware attack?

Scareware

What is scareware?

The term "scareware" refers to malicious computer programs that scare the user into thinking that his or her computer has been damaged or infected with a virus and trick him or her into paying money for a fake antivirus program that often does nothing or actually contains malware. Scareware first appeared in 2009 and it has been growing in popularity among hackers ever since.

Scareware Examples

Some of the most common scareware attacks take the form of pop-up windows that pretend to be messages from an antivirus program, a firewall application or from your Windows operating system. They will typically inform you that your computer has been infected with malware and ask you to purchase an antimalware program to remove the virus. In reality, there is no virus and the

2. Isn't cross-site scripting the user's problem?
3. What can the attacker do with JavaScript?
4. What are the two stages to a typical XSS attack?
5. Can you give some examples of cross-site scriptes?
6. What are the trojans, keylogging and phishing?
7. Can you name the types of Cross-site Scripting attacks?
8. What are the vehicles that are commonly used for Cross-site Scripting attacks?

Task 8. Complete the following sentences using the text.

1. Cross-site Scripting (XSS) is _____injection attack.
2. If an attacker can abuse an XSS vulnerability on a web page to execute arbitrary JavaScript in a user's browser, the security of that vulnerable website or vulnerable web application and its users_____.
3. _____, they are most common in JavaScript, primarily because JavaScript is fundamental to most browsing experiences.
4. Cross-site Scripting may also _____ to deface a website instead of targeting the user.
5. . However, they _____in JavaScript, primarily because JavaScript is fundamental to most browsing experiences.
6. _____can use injected scripts to change the content of the website or even redirect the browser to another web page, for example, one that contains malicious code.
7. The above, in combination with social engineering, allow criminals to pull off advanced attacks including_____, planting trojans, keylogging, phishing, and identity theft.
8. To run malicious _____ code in a victim's browser, an attacker must first find a way to inject malicious code (payload) into a web page that the victim visits.

used within the web page and treated as source code by the victim's browser. There are also variants of XSS attacks where the attacker lures the user to visit a URL using social engineering and the payload is part of the link that the user clicks.

The following is a snippet of server-side pseudocode that is used to display the most recent comment on a web page:

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

The above script simply takes the latest comment from a database and includes it in an HTML page. It assumes that the comment printed out consists of only text and contains no HTML tags or other code. It is vulnerable to XSS, because an attacker could submit a comment that contains a malicious payload, for example:

```
<script>doSomethingEvil();</script>
```

The web server provides the following HTML code to users that visit this web page:

```
<html>
<h1>Most recent comment</h1>
<script>doSomethingEvil();</script>
</html>
```

When the page loads in the victim's browser, the attacker's malicious script executes. Most often, the victim does not realize it and is unable to prevent such an attack.

III. Post-reading activities.

Task 7. Answer the following questions.

1. What is the cross-site scripting?

antimalware program they are trying to get you to purchase is not actually real. In the best-case scenario, you will lose the money you've spent on malware and end up with a bogus program that does nothing. In the worst-case scenario, the newly downloaded program will actually damage your computer or steal your information. Another trick that scareware creators use is that they put a fake "Close" or "X" button somewhere on the Window. When you click the button, it automatically opens a new tab and downloads malware to your computer.

What is the goal of scareware?

There are three things that a scareware program might be trying to achieve. The first one is identity theft – the scareware program will install a malicious key logger program to your device to record everything you type. This will give hackers access to your personal information and passwords. The second goal of scareware software is to get access to your credit card information and scamming you out of money by getting you to pay for a fake antimalware program. Lastly, the third goal of scareware programs is to turn your computer into a "zombie", which means that hackers will gain control over your computer remotely.

What to do during a scareware attack?

Once you've identified that you're under a scareware attack, don't use the "X" or "Close" buttons to close the window, as this may trigger malware to be downloaded to your computer. Instead, close your browser by pressing Ctrl-Alt-Delete of right-clicking the window or tab and selecting "Close". Next, shut down your wireless router and disconnect your computer from the internet. Open your antivirus software and run a full scan to determine if there are any viruses present on your computer. Additionally, check the Quarantine folder in your antivirus program to see if it has discovered any malware before you started the scan. Once you've used your antivirus program to remove all the viruses, restart your computer and make sure that it is running normally. If it's not, it might still be infected with a virus, so it's better to get help from a professional. Finally, it might

be a good idea to contact your bank and let them know that you suspect a scareware attack on your computer to protect yourself from any disputes later.

Джерело: https://hackcontrol.org/blog/what-is-scareware/

III. Post-reading activities.

Task 7. Answer the following questions.

1. What is the goal of scareware?
2. What is the most common example of scareware?
3. Which buttons don't you need to press?
4. Which recommendation do you need to follow during hacker's attack?
5. Why is it useful to contact with bank?
6. What would you do if hackers got access to your personal information?

Task 8. Complete the following sentences using the text.

1. This will give hackers access to your _____ information and passwords.
2. In the worst-case scenario, the _____ program will actually damage your computer or steal your information.
3. Open your antivirus _____ and run a full scan to determine if there are any viruses present on your computer.
4. Scareware first appeared in _____ and it has been growing in popularity among hackers ever since.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

often used to store session tokens. If an attacker can obtain a user's session cookie, they can impersonate that user, perform actions on behalf of the user, and gain access to the user's sensitive data.

- JavaScript can read the browser DOM and make arbitrary modifications to it. Luckily, this is only possible within the page where JavaScript is running.
- JavaScript can use the XMLHttpRequest object to send HTTP requests with arbitrary content to arbitrary destinations.
- JavaScript in modern browsers can use HTML5 APIs. For example, it can gain access to the user's geolocation, webcam, microphone, and even specific files from the user's file system. Most of these APIs require user opt-in, but the attacker can use social engineering to go around that limitation.

The above, in combination with social engineering, allow criminals to pull off advanced attacks including cookie theft, planting trojans, keylogging, phishing, and identity theft. XSS vulnerabilities provide the perfect ground to escalate attacks to more serious ones. Cross-site Scripting can also be used in conjunction with other types of attacks, for example, Cross-Site Request Forgery (CSRF).

There are several types of Cross-site Scripting attacks: stored/persistent XSS, reflected/non-persistent XSS, and DOM-based XSS. You can read more about them in an article titled Types of XSS.

How Cross-site Scripting Works

There are two stages to a typical XSS attack:

1. To run malicious JavaScript code in a victim's browser, an attacker must first find a way to inject malicious code (payload) into a web page that the victim visits.
2. After that, the victim must visit the web page with the malicious code. If the attack is directed at particular victims, the attacker can use social engineering and/or phishing to send a malicious URL to the victim.

For step one to be possible, the vulnerable website needs to directly include user input in its pages. An attacker can then insert a malicious string that will be

malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser. Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.

A web page or web application is vulnerable to XSS if it uses unsanitized user input in the output that it generates. This user input must then be parsed by the victim's browser. XSS attacks are possible in VBScript, ActiveX, Flash, and even CSS. However, they are most common in JavaScript, primarily because JavaScript is fundamental to most browsing experiences.

"Isn't Cross-site Scripting the User's Problem?"

If an attacker can abuse an XSS vulnerability on a web page to execute arbitrary JavaScript in a user's browser, the security of that vulnerable website or vulnerable web application and its users has been compromised. XSS is not the user's problem like any other security vulnerability. If it is affecting your users, it affects you.

Cross-site Scripting may also be used to deface a website instead of targeting the user. The attacker can use injected scripts to change the content of the website or even redirect the browser to another web page, for example, one that contains malicious code.

What Can the Attacker Do with JavaScript?

XSS vulnerabilities are perceived as less dangerous than for example SQL Injection vulnerabilities. Consequences of the ability to execute JavaScript on a web page may not seem dire at first. Most web browsers run JavaScript in a very tightly controlled environment. JavaScript has limited access to the user's operating system and the user's files. However, JavaScript can still be dangerous if misused as part of malicious content:

- Malicious JavaScript has access to all the objects that the rest of the web page has access to. This includes access to the user's cookies. Cookies are

Task 10. Translate from Ukrainian into English.

Що таке Ransomware?

Ransomware використовує шкідливий код, який використовується злочинцями для запуску блокування екрану та атак викрадення даних. Мотив таких атак грошовий, на відміну від інших атак. Жертву повідомлять про подвиг і дадуть інструкції щодо того, як відновитись після нападу. Виплата вимагатиметься у формі віртуальної валюти для захисту особистості злочинця.

Зловмисне програмне забезпечення, що вимагає програмне забезпечення, може поширюватися через вкладення електронної пошти, заражене зовнішнє сховище, заражене програмне забезпечення та скомпрометовані веб-сайти. При атаці на заблокований екран облікові дані жертви можуть бути змінені на комп'ютерному пристрої. При атаці викрадення шкідливе програмне забезпечення буде використовуватися для шифрування файлів на зараженому пристрої та підключених мережевих пристроях. Набори-програми-вимагателі, доступні в Інтернеті, дозволили злочинцям, які володіють незначними технічними знаннями або взагалі не мали їх, купувати програми-вимоглювачі та запускати атаки з дуже незначними зусиллями. Зловмисники використовуватимуть ці методи для вимагання цифрової валюти та експорту цифрових даних своїм жертвам.

Потерпілі отримають спливаючий екран або повідомлення електронною поштою про те, що приватний ключ, необхідний для розблокування пристрою або розшифровки файлів, буде знищений, якщо викуп не буде сплачений. Також жертва може обдурити думку, що вона є предметом офіційного розслідування. Потерпілий буде поінформований про те, що на комп'ютері жертви знайдено нелегальну мережу або неліцензійне програмне забезпечення. Далі слідуватиме інструкція щодо сплати електронного штрафу.

Як захистити себе у таких ситуаціях?

Щоб уберегти себе від таких атак, як вимагання програмного забезпечення та вимагання від користувачів, експерти закликають регулярно оновлювати таке програмне забезпечення, як антивірус, та робити резервні копії комп'ютера. Кінцеві користувачі повинні бути обережними, натискаючи на електронні листи незнайомців та відкриваючи вкладення.

Випадків-нападів не можна повністю уникнути. Існують важливі заходи, які можуть бути вжиті приватними особами та організаціями для мінімізації шкоди та швидкого відновлення. Допоможуть такі стратегії, як зберігання знімків сховища за межами основного пулу зберігання, застосування жорстких обмежень та системи автентифікації відсіків.

Source https://uk.strephonsays.com/scareware-and-vs-ransomware-2703

5. There are also variants of XSS attacks where the attacker lures the user to visit a URL using social engineering and the payload is part of the link that the user clicks.

6. The above, in combination with social engineering, allow criminals to pull off advanced attacks including cookie theft, planting trojans, keylogging, phishing, and identity theft.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. cross site scripting	a) жертва
2. message board	b) непостійний
3. victim	c) законний
4. attacker	d) міжсайтове скриптування
5. non-persistent	e) зловмисний код
6. legitimate	f) зловмисник
7. malicious code	g) дошка оголошень

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What is the cross-site scripting?
2. How can be dangerous about JavaScript?
3. What are the two stages to a typical XSS attack?

Cross-site scripting

Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including

Unit 15. Cross-site scripting

I. Pre-reading activities.

Task 1. How do you understand the statement: *"*The internet is a great way to get on the trap*"* (Bob Dole). **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. How important is cybersecurity?
2. Can you name the most common internet viruses?
3. What do you understand under the term scripting?

Task 3. Try to guess the meaning of the following words.

Web browser, targetting, database, user, attacker, message boards, malicious code,operating system.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.
2. Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.
3. Cross-site Scripting may also be used to deface a website instead of targeting the user.
4. However, JavaScript can still be dangerous if misused as part of malicious content

Unit 9. Kinds of Cyber Crime

I. Pre-reading activities

Task 1.Discuss the following questions.

1. What are the top 5 crimes online?
2. How do you understand the definition "cybercrime" ?
3. Why is cybercrime important?
4. How does cybercrime affect our daily life?
5. How can cybercrime affect you?

Task 2. Try to guess the meaning of the following words.

Exploit, take advantage, to disable a device, dark web, online harassment, to commit an offense, accessibility, internet fraud, card payment data, phishing campaign, to bring down a system.

Task 3. Try to guess from the content what the underlined words and word combinations mean.

1. These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources.
2. Large networks of infected devices known as Botnets are created by depositing malware on users 'computers.
3. They uninstall necessary software in your system including search engines and pre-downloaded apps.
4. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.

5. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.
6. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

Task 4. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. annually	a) вразливість
2. to tackle	b) шкідливе програмне забезпечення
3. to intimidate	c) втручатися
4. malicious	d) щорічно
5. malware	e) залякувати
6. vulnerability	f) зловмисний
7. interfere	g) вирішувати

II While-reading activities.

Task 5. Read the text and answer the questions. Translate the text into Ukrainian

1. What is the most common cyber crime?
2. How cybercrime is being committed?
3. How does cyber crime affect our personal privacy?
4. What is cyber security and how does it affect you?
5. Is cyber crime a social issue?
6. How Social Media Affects cyber security?

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Антивірус, програмне забезпечення, код, системне програмне забезпечення, прикладне програмне забезпечення, інструментальне програмне забезпечення, операційна система, редактор, транслятор, графічний інтерфейс користувача, мікросхема, ліцензія, мова програмування, утиліти, веб програмування, браузер, сервер, база даних, модульне тестування, віджет.

бути направлені на фінансування бюджетних програм та служб на місцевому рівні. Експерти IDC підрахували, що на кожний долар офіційного ПЗ, що продається в країні, припадає $3-$4 прибутку локальним сервісним компаніям-дистриб'юторам. Піратське ПЗ також піддає ризику комп'ютерну безпеку споживачів, оскільки нелегальні програми часто містять шкідливі файли та віруси.

З огляду на все вищевикладене, можна зробити висновок, що Україні терміново потрібні:

- кардинальні зміни в законодавстві у сфері інтелектуальної власності, направлені на боротьбу із Інтернет-піратством (зокрема, зміни до Закону України «Про авторське право і суміжні права» з метою запобігання подальшому збільшенню нелегального використання об'єктів авторського права і суміжних прав в цифровій мережі);
- створення державних програм, направлених на розвиток і підтримку ІТ-галузі вітчизняної економіки;
- укладання державних угод із виробниками і постачальниками програмного забезпечення щодо зменшення вартості ПЗ для українського ринку, як для такого, що розвивається;
- створення спецкурсів у середніх і вищих навчальних закладах, що розтлумачуватимуть необхідність використання ліцензійного програмного забезпечення.

Source: [Електронний ресурс] – Режим доступу: http://conf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iv-konferentsii-2016-g/111-reshtakov

Kinds of Cyber Crime

Cybercrime is vastly growing in the world of tech today. Criminals of the World Wide Web exploit internet users 'personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services. They even gain access to classified government information.

Cybercrimes are at an all time high, costing companies and individuals billions of dollars annually. What's even more frightening is that this figure only represents the last 5 years with no end in sight. The evolution of technology and increasing accessibility of smart tech means there are multiple access points within users 'homes for hackers to exploit. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet.

What is Cybercrime?

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online.

Categories of Cybercrime

There are three major categories that cybercrime falls into: individual, property and government. The types of methods used and difficulty levels vary depending on the category

Types of Cybercrime

DDoS Attacks

These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users 'computers. The hacker then hacks into the system once the network is down.

Botnets

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

Identity Theft

This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.

Cyberstalking

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

Social Engineering

Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

PUPs

PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include

забезпечення та інші об'єкти інтелектуальної власності, невизнання крадіжки об'єкту інтелектуальної власності на одному рівні з крадіжкою об'єкта матеріальної власності;

- недостатній рівень правової та комп'ютерної освіти;
- майже необмежена доступність неліцензійного ПЗ для широкого кола осіб завдяки активному розвитку Інтернет-піратства в Україні.

Відсутність належного правового регулювання, а відтак – реальної відповідальності за використання і розповсюдження неліцензійного ПЗ, мізерні штрафи та неефективні механізми протидії розвитку комп'ютерного піратства призводять до величезних збитків що обчислюються мільйонними, а то і мільярдними сумами, причому збитків зазнає не тільки компанія-правовласник, а й держава, що недоотримує податки. За даними Асоціації виробників програмного забезпечення (Business Software Alliance – BSA) – провідної міжнародної організації, що представляє інтереси індустрії програмного забезпечення та об'єднує такі компанії, як: Acronis, Adobe, Altium, Ansys, Apple, Asseco Poland S.A., Autodesk, Bentley Systems, CGTech, CNC, DBA Lab S.p.A., Microsoft, Siemens, Symantec, Tekla, The MathWorks, VMware тощо, в 2011 році рівень комп'ютерного піратства в Україні сягнув 84%, а загальна вартість неліцензійного ПЗ, встановленого на комп'ютерах користувачів – 647 мільйонів доларів США. Також, згідно даним компанії IDC (International Data Corporation), що є провідною міжнародною компанією в галузі досліджень ринку інформаційних технологій), на кожні $100 офіційного програмного забезпечення, проданого у 2009 році, припадає $75 нелегальних продажів. Ця проблема торкається не лише IT-індустрії, а й економіки в цілому, так як зниження рівня піратства може принести значний економічний зиск. Результати опублікованого в січні 2008 року дослідження впливу рівня піратства на економіку, що було проведене BSA/IDC, показали, що зниження рівня піратства може створити сотні тисяч робочих місць, а також мати ефект для економічного розвитку, що вимірюється в мільярдах доларів і супроводжується зростанням податкових надходжень, що можуть

правопорушення передбачається адміністративна відповідальність за незаконне використання об'єктів права інтелектуальної власності. Також слід згадати статтю 164-9 КУпАП, що встановлює адміністративну відповідальність за незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних, а також статтю 164-13 КУпАП, яка встановлює адміністративну відповідальність за порушення законодавства, що регулює виробництво, експорт, імпорт дисків для лазерних систем зчитування, експорт, імпорт обладнання чи сировини для їх виробництва.

Однак проблематика використання неліцензійного програмного забезпечення є значно ширшою, і полягає не тільки у спектрі юридичному, а й, зокрема, в економічному. Одні з перших випадків використання програмного забезпечення з порушенням авторського права були зафіксовані ще за радянських часів. Тоді, наприкінці 1980-х років, на перші персональні комп'ютери нелегально почали встановлювати модифіковані версії операційної системи MS-DOS, авторськими правами на яку володіє американська корпорація Microsoft. Малорозвинене тогочасне законодавство СРСР у сфері авторського і суміжних прав, а також соціалістичний вектор розвитку держави виключали настання будь-якої відповідальності за такі дії. Після розпаду СРСР і переходу України до капіталістичної економічної системи став можливим правовий захист інтелектуальної власності, в тому числі і на програмне забезпечення. Однак, за роки незалежності нашій державі ще не вдалося суттєво просунутися у сфері легітимізації програмного забезпечення. Серед причин небажання українських компаній і окремих користувачів платити за ліцензійне програмне забезпечення можна виділити наступні:

- висока вартість програмного забезпечення у співвідношенні до порівняно невисокого рівня прибутків на душу населення в Україні;
- відсутність у правовій свідомості і правовому менталітеті більшості українців розуміння необхідності платити за програмне

spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.

Phishing

This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

Prohibited/Illegal Content

This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

Online Scams

These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

Exploit Kits

Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user's computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

Джерело: https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/

III. Post-reading activities.

Task 6. Complete the following sentences using the text.

1. The evolution of technology and increasing accessibility of smart tech means there are multiple access points within users 'homes for hackers to exploit.
2. They can also open a phone/internet account in your name, use your name to plan a criminal activity and _____ government benefits in your name.
3. They want _____ your confidence and usually pose as a customer service agent so you'll give the necessary information needed.
4. _____ are becoming more established and many of these emails are not flagged as spam.
5. Illegal content includes materials advocating _____ acts and child exploitation material.

Task 7. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 8. Translate from Ukrainian into English.

Як захиститися від кіберзлочинності?

Кожен, хто користується Інтернетом, повинен дотримуватися деяких основних запобіжних заходів. Ось 7 порад, якими ви можете захиститися від різноманітних кіберзлочинів.

1. Використовуйте повний пакет послуг Інтернету

Наприклад, Norton Security забезпечує захист у режимі реального часу від існуючих та нових шкідливих програм, включаючи програми-вимагателі

8. There are _____ of softwares which include system software dealing with the _____of the computers, the application softwares dealing with computation process and the programming software for the programmers to develop a software by writing programming language in it.

9. Rise of internet during 1980s witness the rise of new kind of software piracy when thieves use dial-up _____used to upload and download software to computer owners.

10. There are many organizations fighting against the piracy the eminent one is _____set up in 1988.

Task 9. Make a list of all the terms you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Використання неліцензійного («піратського») програмного забезпечення є одним з видів порушення авторського права, що у певних випадках визнається кримінальним правопорушенням. Юридичні словники дають цьому явищу назву «контрафакція». Російський вчений С.П. Гришаєв визначає порушення авторського права як правопорушення, суть якого полягає у використанні витворів науки, літератури і мистецтва, що охороняються авторським правом, без дозволу авторів або правовласників або з порушенням умов договору про використання таких витворів.

Кримінальний кодекс України встановлює відповідальність за порушення авторських і суміжних прав у статті 176; відповідальність настає за незаконні відтворення, розповсюдження чи інше використання творів, які є об'єктом авторського права, без дозволу авторів, якщо ці дії спричинили шкоду у значному розмірі (понад 20 неоподатковуваних мінімумів доходів громадян). Крім того, у статті 51-2 Кодексу України про адміністративні

4. What percentage of software is unlicensed and unauthorized around the world?
5. What inventions and technologies caused major development of the world?
6. Are there many organizations fighting against the piracy?
7. How did piracy appear?
8. What are three main types of software?
9. What does the word `spyware` mean?
10. What is the punishment for unlicensed using of the software?

Task 8. Complete the following sentences using the text.

1. The _____which is digitally signed by the licensee as "I agree" is a trust that the licensee will not make multiple copies of the software and sale it or give it to other users who has not been authorized by the licensor.

2. Although all the computer users are aware of _____ and their repercussions but piracy still exists as a global concern around the world.

3. Since the economy of the country is now dependent upon such computer technologies there is a dire need for the protection of _____through law.

4. There is a _____conducted among the 20,000 users and enterprise users of the personal computers which showed that 43 per cent of software which is installed in the PC is unlicensed and unauthorized around the world in _____.

5. The survey was conducted as an initiative naming "_____" by Business Software Alliance partnership with International Data Corporation.

6. The world has seen major _____due to these inventions and advancement of technologies.

7. The computer software programs are also included in the original works of the _____and are one of the fast-growing segments in the economy of the country and thus protected under the Indian Copyright Act and Information Technology Act.

та віруси, а також допомагає захистити вашу приватну та фінансову інформацію, коли ви перебуваєте в Інтернеті.

2. Використовуйте надійні паролі

Не повторюйте свої паролі на різних сайтах і регулярно змінюйте їх. Зробіть їх складними. Це означає використання комбінації принаймні з 10 букв, цифр та символів. Програма управління паролями може допомогти вам утримувати ваші паролі заблокованими.

3. Оновлюйте програмне забезпечення

Це особливо важливо для ваших операційних систем та програмного забезпечення для захисту Інтернету. Кіберзлочинці часто використовують відомі подвиги або вади вашого програмного забезпечення, щоб отримати доступ до вашої системи. Виправлення цих подвигів та вад може зменшити вірогідність того, що ви станете об'єктом кіберзлочинності.

4. Керуйте налаштуваннями соціальних мереж

Тримайте вашу особисту та приватну інформацію заблокованою. Кіберзлочинці соціальної інженерії часто можуть отримати вашу особисту інформацію лише за допомогою декількох точок даних, тому чим менше ви публічно ділитесь, тим краще. Наприклад, якщо ви опублікуєте прізвище вашого улюбленця або відкриєте дівоче прізвище матері, ви можете запропонувати відповіді на два поширені питання безпеки.

5. Поговоріть зі своїми дітьми про Інтернет

Ви можете навчити своїх дітей прийнятному використанню Інтернету, не вимикаючи каналів зв'язку. Переконайтесь, що вони знають, що можуть звернутися до вас, якщо вони зазнають будь-яких переслідувань в Інтернеті, переслідування чи залякування.

6. Будьте в курсі основних порушень безпеки

Якщо ви працюєте з продавцем або маєте обліковий запис на веб-сайті, на який вплинуло порушення безпеки, з'ясуйте, до якої інформації хакери отримували доступ, і негайно змініть свій пароль.

7. Слідкуйте за дітьми

Подібно до того, як ви захочете поговорити зі своїми дітьми про Інтернет, ви також хочете допомогти їм захистити їх від крадіжки особистих даних. Злодії особистості часто націлюються на дітей, оскільки їх номер соціального страхування та кредитна історія часто являють собою чистий аркуш. Ви можете допомогти захиститися від викрадення особистих даних, дотримуючись обережності, передаючи особисту інформацію дитини. Також розумно знати, на що звертати увагу, що може припустити, що особистість вашої дитини порушена.

Task 9. Give the Engish equivalents of the Ukrainian words and word combinations.

Програмне забезпечення, викрадення особистих даних, економічна вигода, обліковий запис, залякування, переслідування в Інтернеті, заблоковані паролі, канали зв'язку, порушення безпеки, особисті дані, доступ в Інтернеті, соціальне страхування, шахрайство.

technologies, the world saw the rise of intermediaries which where the single users of the softwares and they used to do their customers jobs by installing the softwares in everyone's computers through floppy disks and CDs through process called mail trading thus giving rise to piracy.

Rise of internet during 1980s witness the rise of new kind of software piracy when thieves use dial-up Bulletin Board Systems used to upload and download software to computer owners. They log on to telephone connections, download softwares and trade floppy disks via mail system. The activity was so complex during the time that law enforcement could do nothing to curb the theft and off course the law was not much advance. The BBS systems distribute the software for free or less money. The advance of internet during 90s gave rise to more distinct form of stealing such as hacking. The new form of systems such as Relay chats, creation of public mailbox, File Transfer Protocol which allows computers to store and share data from one computer to another made the piracy easy. There are many organizations fighting against the piracy the eminent one is Business Software Alliance an NGO set up in 1988. The BSA represents world class software makers with aim to protect infringement of copyright software around the world. With the aim of promoting legal environment and standard in which software industries can thrive the BSA make laws in compliance with international treaties.

Source: [Електронний ресурс] – Режим доступу : https://blog.ipleaders.in/ipr-software-privacy/

III. Post-reading activities.

Task 7. Answer the following questions.

1. What does the word `software piracy` mean?
2. Why does piracy still exist as a global concern around the world?
3. Why is it a dire need for the protection of copyrighted materials?

Information Technology Act. There is also patent protection given by certain countries such as the USA and Japan for the protection of copyrighted softwares.

Computer software programs is made through programming languages which enable it to hold a collection of data which prescribed certain instructions to the computers for action which has to be done or not to be done, in manners in which it has to be done according to the command given by the users of the software. The programming language which is compiled together and made as the software is created by the programmer or operator and is then transferred into the language understandable by the computer. It is thus the list of instruction which user of the software desire to be done by the computer. There are three types of softwares which include system software dealing with the hardware components of the computers, the application softwares dealing with computation process and the programming software for the programmers to develop a software by writing programming language in it. These softwares are available to the users by way of freeware, payware, shareware and sometimes open source.

Evolution of Piracy through rise of Internet

There is misconception that software piracy is the now criminal activity attributed to the advancement of technologies and use of Internet but it is evident that piracy is much older and in fact was easy as during the 60s the developer sale the computer softwares along with the computer hardware which makes them easy to be steal. But after the technological advancement and use of software in almost everything has caused separate creations and selling of softwares by respective separate software companies. These companies give license to the users who purchase the software violating to which the infringement of copyright takes place. In older days the copyright was only given to the code which is used to create a software as during that time only the copying of the code by the competitors where prevalent. There was no concept of software piracy. The code which is used to create software cannot be used as creating another software. These codes include object code, source code and documentation and the copyright law was protecting only the above mentioned codes. After few decades of the advancement of

Unit 10. Cyber Stalking

I. Pre-reading activities

Task 1. How do you understand the difference between the terms *cyberstalking* and *harassment*

Task 2. Discuss the following questions.

1. What does cyberstalking mean?
2. Is there a legal definition of cyberstalking?
3. How can you stop cyberstalking?

Task 3. Try to guess the meaning of the following words.

Victim , false accusations, engage in identity theft, spyware, social media profiles, cautious, responsible for, to verify, basic security, to insure, log out, log in, a big clue, separate folder, dating site.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. While most cyberstalking victims are women, 20 to 40 percent of victims are actually men.
2. Cyberstalking can include other behavior that's intended to intimidate victims or make their lives unbearable.
3. Cyberstalkers have been known to fit GPS devices to their victims' cars, use geolocation spyware on their phones, and obsessively track their victims' whereabouts through social media.
4. You may be shocked by how easy it is to track you down.

5. Take a good look at your social media accounts and if you haven't done already, enable strong privacy settings.
6. Use a gender-neutral screen name or pseudonym for your social media accounts — not your real name.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. to intimidate	a) запит
2. to hack	b) зламати
3. malicious	c) вибірковий
4. optional	d) зловмисний
5. rumors	e) приймати
6. to accept	f) залякувати
7. request	g) чутки

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian

1. What is cyberstalking?
2. What to do in case you are being cyberstalked?
3. How do cyberstalkers get started?
4. Is it important to increase your privacy setting ? Why?
5. How to avoid being stalked online?

showed that 43 per cent of software which is installed in the PC is unlicensed and unauthorized around the world in 2013. The total loss which is credited due to such unlicensed instalment of copyrighted software is more than 60 billion in dollars. The survey was conducted as an initiative naming “Global Software Survey” by Business Software Alliance partnership with International Data Corporation. This survey was alarming for the government around the world to make stringent laws for the protection of copyrighted softwares. In India, both Judiciary and Legislative authorities is constantly fighting against this curable disease by judicial approach and Acts such as Indian Copyright Act and IT Act and there amendments in compliance with International treaties respectively.

Software Piracy in India

Conflicts on availability of Computer Softwares

Due to advancement of technology, digitalisation widespread use of internet the manual works has been completely transformed into technological work. The world has become significantly small in a single click of the computer. All the information is available on the internet. The world has seen major development due to these inventions and advancement of technologies. This technology has brought significant change in everyone’s life around the world as business and commerce to which the economy of a country is depended is now itself depended upon a software. This advancement has though enabled everything but has brought many problems with it. The usage of internet has been successfully helping in all kinds of research but has brought complex problems especially in the field of cyber laws and infringement laws with it. Infringement of copyrighted software also known as piracy is the most common but complex problem which had been generated by such development of the technology. The copyright laws aim to protect original/literary works created by its creator/owner these works include cinematographic tapes, sound recordings, musical and dramatic works, films and literary works. The computer software programs are also included in the original works of the creator/owner and are one of the fast-growing segments in the economy of the country and thus protected under the Indian Copyright Act and

ongoing digitalization and technological advancement draw concern of the government to make laws governing infringement of such works. Modern problems such as illegal duplication and distribution of the original work like software have a significant impact on the economy. The copyright infringement of these computer programs means unauthorized copying of software programs through hacking or any other means, selling those duplicated programs in the market. These pirated works cause damage to not only its developers but also their users. The paper thus explains the ongoing menace of the software piracy in India, the online piracy of software programs, hacking and laws and mechanisms to protect such crime as well as judicial approach. The paper will emphasize the Indian Copyright Act and Information Technology Act as well as their compliance with the international treaties.

Software piracy is defined as a crime relating to illegal copying/duplicating, selling or installing of the copyrighted software. However many jurisprudence also includes copying of programs and codes of copyrighted software to develop new software also as piracy. The copyrighted software is generally a license which the licensor sale to the licensee for a certain amount which can only be used by the single authorized user who has purchased the license. This software can be used in two or more devices as long as the licensee is only the user. The license terms and agreement which is digitally signed by the licensee as “I agree” is a trust that the licensee will not make multiple copies of the software and sale it or give it to other users who has not been authorized by the licensor. If the licensee does the above-mentioned act this will amount to a violation of license terms and agreement and these defeat of trust will amount to software piracy. Although all the computer users are aware of software piracy and their repercussions but piracy still exists as a global concern around the world. Like any other infringement of copyrighted work, piracy is also defeating the creativity. Since the economy of the country is now dependent upon such computer technologies there is a dire need for the protection of copyrighted material through law. There is a survey conducted among the 20,000 users and enterprise users of the personal computers which

Cyber Stalking

What is cyberstalking?

Cyberstalking's definition is quite simply, “the use of the internet, or other electronic means, to harass and intimidate a selected victim”.

Common characteristics include (but aren't limited to) classic 'stalking' behavior – tracking someone's location and monitoring their online and real-world activities. Cyberstalkers have been known to fit GPS devices to their victims' cars, use geolocation spyware on their phones, and obsessively track their victims' whereabouts through social media.

Cyberstalking can include other behavior that's intended to intimidate victims or make their lives unbearable. For instance, cyberstalkers might target their victims on social media, trolling and sending threatening messages; they might hack emails, to communicate with the victim’s contacts, including friends and even employers. Social media stalking can include faking photos or sending threatening private messages. Often, cyberstalkers will spread malicious rumors and make false accusations, or even create and publish revenge porn. They might also engage in identity theft and create fake social media profiles or blogs about their victim.

So, we know what cyberstalking is. But who are its victims? You might be surprised. While most cyberstalking victims are women, 20 to 40 percent of victims are actually men.

Cyberstalking goes a lot further than just following someone on a social network. It's the intent to intimidate, which is the defining characteristic of cyberstalking.

How to avoid being stalked online

One good exercise you should carry out now is to Google yourself and find out just what information a potential cyberstalker could find online. You may be shocked by how easy it is to track you down. Not to mention, find your home address, phone number, and other personal details.

And if that's bad, you might want to check how much data someone could compile on you if they had access to your friends' and family's social media, too. For instance, they might find out which bar you were in, with which friends, or where you'll next be going on holiday and when.

You might even find stuff purporting to be from you that someone else has uploaded: a fake blog, or a Craigslist account putting your phone number and home address out there.

This is how cyberstalkers get started - Googling their victims and finding out everything they can. That means you'll certainly want to make that information as hard to obtain as possible.

Tips for protecting yourself from cyberstalkers

Increase your privacy settings

Start off with your own data. Take a good look at your social media accounts and if you haven't done already, enable strong privacy settings.

- Make your posts 'friends only' so that only people you know get to see them.
- Don't let social networks post your address or phone number publicly. (You might even want to have a separate email address for social media)
- If you need to share your phone number or other private information with a friend, do so in a private message - not in a public post.
- Use a gender-neutral screen name or pseudonym for your social media accounts — not your real name
- Leave optional fields in social media profiles, like your date of birth, blank.
- Only accept friend requests from people you have actually met in person. Set your social networks to accept friend requests only from friends of friends.
- Disable geolocation settings. You may want to also disable GPS on your phone.

5. These softwares are available to the users by way of freeware, payware, shareware and sometimes open source.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. operating system	a) код
2. program	b) шпигунське програмне забезпечення
3. developer	c) забезпечення
4. implementation	d) мережа
5. network	e) операційна система
6. code	f) програма
7. spyware	g) розробник

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What is the system of software designed for?
2. Why is unlicensed software very common?
3. How to resist its spreading?

Software piracy and crime related to IPRS

There is legal protection given to the creators of works originally created by him/her under Indian Laws. This literary/original work includes computer programs and compilations, languages, websites and web pages designed by the creator, databases, software codes/schemes and any other form of material. The

Unit 14. Software piracy and crime related to IPRS

I. Pre-reading activities.

Task 1. How do you understand the statement: *"The sure way to be cheated is to think one`s self more cunning than others"* (La Rochefoucauld). **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What does the word `software` mean?
2. What types of software do you know?
3. What are the most common problems related to the software?

Task 3. Try to guess the meaning of the following words.

Software engineering, waterfall model, bundled software, software development, software release life cycle, application software.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. Software piracy is defined as a crime relating to illegal copying/duplicating, selling or installing of the copyrighted software.
2.Many jurisprudence also includes copying of programs and codes of copyrighted software to develop new software also as piracy.
3. Due to advancement of technology, digitalisation widespread use of Internet the manual works has been completely transformed into technological work.
4. They log on to telephone connections, download softwares and trade floppy disks via mail system.

If other personal data is up on the web outside your social media accounts, start removing it. In the case of your SSN being displayed, Google will help you remove that. You may need to contact third party websites to get some of the data taken down. If you need a postal address for business, or for registering your web domain, use a post box address or office address (like your accountant's, for instance), not that of your home.

Джерело: https://www.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking

III. Post-reading activities.

Task 7. Complete the following sentences using the text.

1. _____ can include other behavior that's intended to intimidate victims or make their lives unbearable.
2. Take _____ your social media accounts and if you haven't done already, enable strong privacy settings.
3. That _____ you'll certainly want to make that information as hard to obtain as possible.
4. Use a gender-neutral screen name or pseudonym for your social media accounts — not your _____.
5. Disable _____ settings.
6. You may want to also disable _____ on your phone.
7. You may need to contact _____party websites to get some of the data taken down.

Task 8. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 9. Translate from Ukrainian into English.

Вплив переслідування на жертв

Жертви переслідування є багатим джерелом інформації, що сприяє не лише нашому розумінню досвіду тривалих домагань, але й нашим знанням про переслідування в цілому. Завдяки широкомасштабним опитуванням громади та меншим дослідженням конкретних груп жертв ми почали розуміти шкідливі та потенційно руйнівні наслідки переслідування віктимізації. Окрім частих юридичних передумов страху та можливості поранення внаслідок нападу, дослідження показали, що жертви зазнають широкого спектру психологічних, фізичних, професійних, соціальних та загальних наслідків способу життя як наслідок переслідування. Як і у випадку з багатьма аспектами переслідування, досвід та вплив можуть сильно відрізнятися між жертвами з поведінкою, яка може вважатися досадною для однієї жертви, може мати руйнівний ефект для іншої.

Який вплив стеження за жертвами?

Вплив переслідування може різнитися залежно від характеристик жертви, минулого досвіду, поточних обставин та того, що вони знають або не знають про сталкера. Те, як інші реагують на ситуацію жертви, включаючи те, як влада керує переслідуванням, може вплинути на загальний вплив епізоду переслідування на жертву. Незважаючи на складність, яка може відрізнятися від досвіду та реакції людини на переслідування, дослідження продемонстрували загальні моделі реагування. Хоча жінки-жертви зазвичай повідомляють про більший рівень страху, дослідження показали, що чоловіки, які зазнають переслідування, відчувають симптоми, подібні до тих, що повідомляють їх колеги-жінки.

Нижче наведено деякі найпоширеніші наслідки, які стикаються з жертвами переслідування:

Вплив на психічне здоров'я

оголені фото, що нерідко стають предметом шантажу, і навіть влаштовують реальні зустрічі, які можуть закінчитися розбещенням, переслідуванням, зґвалтуванням тощо.

І хоча в закладах загальної середньої освіти ведеться робота серед учнів у напряму підвищення обізнаності про кібербезпеку, але в той же час є необхідність більш детального вивчення питання безпечного поводження в Інтернеті з практичними заняттями, про що повідомили 52% опитаних школярів.

Слід зазначити, що для полегшення виявлення та розкриття, а також запобігання злочинам відносно дітей у сфері моральності та пов'язаних з ними злочинам, що посягають на статеву свободу та статеву недоторканість, необхідно вирішення таких завдань: − добитися криміналізації володіння, придбання, одержання доступу, зберігання матеріалів, що містять дитячу порнографію, відповідно міжнародним нормативно-правовим актам; − налагодити навчання дітей правилам безпечної поведінки в глобальній мережі Інтернет.

Source: [Електронний ресурс] – Режим доступу : http://www.lsej.org.ua/5_2020/45.pdf?fbclid=IwAR1QpCbG8c50vxR33NwHHc4iabeFtLf-k3L1NpiKUxPGjJHIIS6BXOiu_7U

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Сексуальна експлуатація дітей, тіньовий порнобізнес, сексуальне домагання, схиляння до самогубства, шантаж, переслідування, залякування, сексуальне домагання, розбещення, кримінальна діяльність, інтернет-злочинці, насильницький контент, жертва злочинних посягань, викрадення дітей, система нормативно-правових актів, міжнародний правовий акт.

сексуальної експлуатації дітей. Було наголошено, що Україна входить до п’ятірки найбільших виробників дитячої порнографії в світі.

Одночасно величезні доходи від тіньового порнобізнесу стимулюють розвиток іншої кримінальної діяльності в мережі Інтернет. Зокрема, незаконний порнобізнес дає роботу великій кількості хакерів і програмістів, що пишуть вірусні програми, оскільки для приховування своєї діяльності від правоохоронних органів організатори нелегальних сайтів часто користуються їх послугами. Таким чином, злочинна діяльність з використанням всесвітньої мережі постійно вдосконалюється.

У зв’язку з тим, що дитяча порнографія в мережі інтернет розповсюджується легко, швидко та дешевше, ніж цифрове телебачення, то в основному злочинці й використовують саме її. З іншого боку, інформаційно-комунікаційні технології можуть використовуватися і для встановлення контакту із дітьми, дуже часто з метою подальшої сексуальної експлуатації. Зробити це доволі просто, враховуючи те, що сучасні діти не розділяють світ на цифровий (віртуальний) та реальний, інтернет все частіше стає засобом їх соціалізації. Зокрема, реєстрація у соцмережах – це наслідок природньої потреби дитини перебувати у групі за уподобанням, наголошують психологи. Отже, підлітки використовують Всесвітню мережу передусім для спілкування, розширення кола знайомих тощо.

Небезпека полягає в тому, що велика ймовірність під час віртуального знайомства та спілкування стати жертвою шантажу, переслідувань, залякувань, сексуальних домагань, схиляння до самогубства тощо. Ситуація ускладнюється ще й тим, що діти через свій вік, відсутність життєвого досвіду та стійкої здатності критично мислити легко йдуть на контакт у соцмережах, повідомляють особисту інформацію, діляться власними фото (часто відвертого характеру) тощо.

Інтернет-злочинці в своєму арсеналі мають десятки схем, як завдяки соцмережам впливати на неповнолітніх. Часто вони, реєструючись під вигаданими іменами, спілкуються з дітьми, виманюють особисті дані,

- Заперечення, розгубленість, невпевненість у собі, сумніви, чи нерозумно те, що відбувається, цікавляться, чи надмірно вони реагують
- Провина, збентеження, самозвинувачення
- Побоювання, страх, жах залишитися наодинці або що їм, іншим чи домашнім тваринам буде заподіяно шкоду.
- Відчуваючи себе ізольованим і безпорадним, щоб зупинити переслідування
- Депресія (всі симптоми, пов'язані з депресією)
- Тривога, напади паніки, агорафобія (злякавшись вийти з дому, ніколи не почуваючись в безпеці)
- Труднощі з концентрацією уваги, відвідуванням та запам’ятовуванням речей
- Неможливість заснути – нічні жахи
- Дратівливість, гнів, думки про вбивства
- Емоційне оніміння
- Симптоми посттравматичного стресового розладу, наприклад гіпер пильність (завжди на сторожі), спалахи лякаючих випадків, які легко лякають
- Невпевненість і неможливість довіряти іншим, проблеми з близькістю
- Особистість змінюється внаслідок того, що стає більш підозрілим, замкнутим в собі або агресивним
- Самолікування алкоголем / наркотиками або використання призначених ліків
- Думки про самогубство та / або спроби самогубства

Task 10. Give the Engish equivalents of the Ukrainian words and word combinations.

Напади паніки, нездатність довіряти людям, змінювати зовнішній вигляд, ізольований, нічні жахи, страх, заподіяти шкоду, симптоми, дослідження показати, довіряти, самогубство, жертвувати, уникати.

Task 10. Translate from Ukrainian into English.

На цей час за оцінками зарубіжних експертів дитяча порнографія за прибутком посідає у світі третє місце після торгівлі наркотиками і зброєю. Зауважимо, що 68 мільйонів пошукових запитів на день у мережі Інтернет пов'язані з порнографією (у тому числі дитячою). Тобто інтернет-ресурси пропонують найрізноманітніший контент з використанням усіх можливих способів його доставки. На вибір зацікавленого користувача пропонуються фотографії та відео зі сценами сексуального насильства над реальними дітьми з будь-якої країни.

Підтвердженням є статистика міжнародних організацій. Зокрема, кожні 5 хвилин Internet Watch Foundation*1 знаходить в Інтернеті фото чи відео із сексуальним насильством над дитиною (дитячою порнографією), 40% з них містять зображення дітей молодших десяти років. Вартість онлайн-трансляції сексуального насильства над дитиною становить близько 10–20 євро.

Слід вказати на те, що проблема дитячої проституції притаманна будь-якій країні незалежно від її географічного розташування, соціально-економічного рівня розвитку та політичної системи управління тощо. Наприклад, за даними опитування в Таїланді, 92% дітей, що розмовляли в чаті, мали запрошення поговорити про секс. 20% дітей віком від 7 до 11 років, які спілкувалися в чаті, відзначили травмуючий досвід, коли вони зіткнулися з нецензурною лексикою (34%) та коли їм запропонували переслати матеріали про насильство чи секс (66%). У 58% випадків зустріч з «другом» була неприємним сюрпризом, тому що діти зрозуміли, що їхній віртуальний «друг» брехав про себе.

З роками ситуація не поліпшується. У лютому поточного року уповноважений президента України з прав дитини М. Кулеба зазначив, що за офіційними даними, щоденно близько 3 000 осіб на території України здійснюють розповсюдження порнографічних матеріалів із зображенням

Task 8. Complete the following sentences using the text.

1. Images were usually locally produced, _____, expensive, and difficult to obtain.
2. Despite concern about the extent of child pornography, _____had considerable success in stemming the trafficking of these traditional hard-copy forms.
3. The advent of the Internet in the 1980s dramatically changed the scale and nature of the_____, and has required new approaches to investigation and control Internet child pornography is unlike most crimes local police departments handle.
4. Local citizens may access child pornography images that were _____and/or stored in another city or on another continent.
5. Most of the major investigations of Internet child pornography have involved cooperation among_____, often at an _____.
6. However, within this broader scheme, local police departments have a _____to play.
7. By concentrating on components of the problem that occur within their local jurisdictions, they may uncover _____that initiates a wider investigation.
8. Because of the increasing use of computers in _____, most police departments are likely to encounter Internet child pornography crimes.
9. It would be a mistake to underestimate the importance of _____in detecting and preventing Internet child pornography offenses.
10. One study found that _____of arrests for Internet child pornography crimes originated from non-specialized law enforcement agencies.

Task 9. Make a list of all the terms you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Unit 11. rgery and counterfeiting

I. Pre-reading activities.

Task 1. How do you understand the statement: *"Honesty is the best policy".* **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. Can you name the identity documents?
2. Does each country tend to have a list of "state approved" identity documents?
3. Why is it difficult to detect false documents?

Task 3. Try to guess the meaning of the following words.

Identity document, false document, ID card, driver`s license, unlawful activity, falsification.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. The unique features of many identity documents make it very hard for criminals to create false copies in order to steal someone's identity or carry out unlawful activity.
2. Forgery is the crime of producing illegal copies of documents with the intent to defraud.
3. A person is guilty of forgery if they alter any writing or makes any writing of another person and proclaims it to be the act of the other person who did not actually authorise the act.

4. A counterfeit is something which is ‘made to look like the original of something, usually for dishonest or illegal purposes’.

5. The unauthorized reproduction of coins has been a craftsmanship that could only be done by blacksmiths who actually used to work at a blacksmith-shop or forgery.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. counterfeit	a) відтворення
2. forgery	b) діяльність
3. craftmanship	c) шахрайство
4. fraud	d) підробка
5. activity	e) дані
6. reproduction	f) фальшивка
7. data	g) майстерність

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. How can you reveal false documents?
2. What you should do when you reveal false documents?
3. What is the punishment for false documents?

Forgery and counterfeiting

Here, we will explore the difference between the terms and what they mean in practice when referring to falsified identity documents.

- Makes pornography instantly available at any time or place
- Allows pornography to be accessed (apparently) anonymously and privately
- Facilitates direct communication and image sharing among users
- Delivers pornography relatively inexpensively
- Provides images that are of high digital quality, do not deteriorate, and can be conveniently stored
- Provides for a variety of formats (pictures, videos, sound), as well as the potential for real-time and interactive experiences
- Permits access to digital images that have been modified to create composite or virtual images (morphing).

Source: [Електронний ресурс] – Режим доступу : https://popcenter.asu.edu/content/child-pornography-internet-0

III. Post-reading activities.

Task 7. Answer the following questions.

1. What are the kinds of abuse against children?
2. Can pornography be addictive?
3. Does viewing child pornography affect the mental state?
4. Who should investigate crimes related to pornography?
5. How do you think this process works?
6. What is the role of the Internet in promoting child pornography?
7. Why is it impossible to stop the spreading of child pornography?
8. What consequences can be for victims of abuse?
9. Is child pornography prevalent in your country?
10. How can people resist abuse against children?

crimes. Therefore, it is important that all police departments develop strategies for dealing with the problem. Larger departments or districts may have their own dedicated Internet child pornography teams, but most smaller ones do not, and the responsibility for day-to-day investigations will fall to general-duties officers. It would be a mistake to underestimate the importance of local police in detecting and preventing Internet child pornography offenses. One study found that 56 percent of arrests for Internet child pornography crimes originated from non-specialized law enforcement agencies.

Related Problems

Internet child pornography is only one of a number of problems related to either child abuse or the Internet. Other related problems not directly addressed by this guide include:

- Violence and fatalities
- Neglect
- Abandonment
- Exposure to hazardous materials (e.g., clandestine drug labs)
- Trafficking of children and babies and illegal adoption agencies
- Juvenile runaways
- Internet Crime
- Online solicitation of children for sexual activity
- Identity theft (sometimes known as phishing)
- Hacking.
- Child Abuse

The Role of the Internet in Promoting Child Pornography

The Internet has escalated the problem of child pornography by increasing the amount of material available, the efficiency of its distribution, and the ease of its accessibility. Specifically, the Internet:

- Permits access to vast quantities of pornographic images from around the world

There are thousands of identification documents in circulation worldwide. Identity documents can take many forms – from ID cards, to driver's licenses, to passports and digital IDs – and it is crucial that each one is unique and has specific features that allow it to be verified.

The unique features of many identity documents make it very hard for criminals to create false copies in order to steal someone's identity or carry out unlawful activity. The rarer an identity document is, the better it is at protecting its holder.

Each country tends to have a list of 'state-approved 'identity documents that are rare, unique and protected enough to be trusted by financial institutions and when carrying out sensitive activity. All countries have passports but each is unique and special in some way. They come in different colours and textures, containing differing content, and are considered to have varying levels of power depending on how many countries they allow the carrier to enter.

Forgeries

Forgery is the crime of producing illegal copies of documents with the intent to defraud. A person is guilty of forgery if they alter any writing or makes any writing of another person and proclaims it to be the act of the other person who did not actually authorise the act.

Fake, forgery and counterfeit all mean an item is not genuine, but forgery and counterfeit implies intentional illegality.

- **Counterfeits**

A counterfeit is something which is 'made to look like the original of something, usually for dishonest or illegal purposes'.

Although the term counterfeit is generally associated with making, dealing, or possessing any counterfeit currency, it also includes forgeries of documents and imitations of goods and trademarks. In the case of goods, counterfeiting results in patent infringement or trademark infringement. Making, dealing, or possessing any plate, stone, analog, or any other thing, or part used for counterfeiting also amounts to the crime.

- **Forgery vs. Counterfeit**

Forgery comes from the verb to forge. To forge an object means that you fabricate by working, heating, hammering and shaping it into a certain shape.

Counterfeit contains the noun 'feit' that means something as 'fact' and originates in Middle Dutch. In other words, forgery contains the act of recreating, where counterfeit expresses the result of forgery and it's value - non-genuine.

Forgery could be seen as a craftsmanship, it involves techniques, work and mastery and often is of quality, it's well done. On the contrary counterfeit lacks quality all together. Counterfeit on the could be seen as a value statement, it involves, quality is not involved.

- **Why is the act of forgery then connected to the result of counterfeit?**

Usually the word forgery is used when we speak about the unauthorized reproduction of valuable documents or objects where the value is determined not by the actual document but the social or mutual agreement or culture, such as an agreement, art, or money. Unauthorized is the keyword here.

The unauthorized reproduction of coins has been a craftsmanship that could only be done by blacksmiths who actually used to work at a blacksmith-shop or forgery. A reproduction of of coins therefore would be called a forged, and it being done unauthorized would render these coins factually worthless - counterfeit.

- **How We Can Help**

Depending on their sophistication, false documents can be difficult to detect when used to verify identity and manual identity verification checks are not just time consuming, but also produce a lengthy and clunky onboarding process for customers.

The challenge is to verify the authenticity and information on identity documents without adding unnecessary time to the onboarding process. This is where our automated solutions come to the fore.

Our leading solution for global document verification, iDocufy utilises a global database of over 5,000 forms of government-issued identity documents to

problem. Finally, it reviews responses to the problem and what is known about these from evaluative research and police practice.

The treatment of children as sexual objects has existed through the ages, and so too has the production of erotic literature and drawings involving children. However, pornography in the modern sense began with the invention of the camera in the early nineteenth century. Almost immediately, sexualized images involving children were produced, traded, and collected. Even so, child pornography remained a restricted activity through most of the twentieth century. Images were usually locally produced, of poor quality, expensive, and difficult to obtain. The relaxation of censorship standards in the 1960s led to an increase in the availability of child pornography, and, by 1977, some 250 child pornography magazines were circulating in the United States, many imported from Europe. Despite concern about the extent of child pornography, law enforcement agencies had considerable success in stemming the trafficking of these traditional hard-copy forms. However, the advent of the Internet in the 1980s dramatically changed the scale and nature of the child pornography problem, and has required new approaches to investigation and control.Internet child pornography is unlike most crimes local police departments handle. Local citizens may access child pornography images that were produced and/or stored in another city or on another continent. Alternatively, they may produce or distribute images that are downloaded by people thousands of miles away. An investigation that begins in one police district will almost certainly cross jurisdictional boundaries. Therefore, most of the major investigations of Internet child pornography have involved cooperation among jurisdictions, often at an international level.

However, within this broader scheme, local police departments have a crucial role to play. By concentrating on components of the problem that occur within their local jurisdictions, they may uncover evidence that initiates a wider investigation. Alternatively, they may receive information from other jurisdictions about offenders in their districts. Because of the increasing use of computers in society, most police departments are likely to encounter Internet child pornography

5. Larger departments or districts may have their own dedicated Internet child pornography teams, but most smaller ones do not, and the responsibility for day-to-day investigations will fall to general-duties officers.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. jurisdiction	a) рентабельність
2. abandonment	b) усиновлення
3. adoption	c) цифрове зображення
4. accessibility	d) судочинство
5. digital image	e) злом
6. hacking	f) відмова
7. efficiency	g) доступність

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. When did pornography become widely distributed?
2. What are the types of child abuse?
3. How does child pornography affect society?

Child pornography

The guide begins by describing the problem and reviewing factors that increase the risks of Internet child pornography. It then identifies a series of questions that might assist you in analyzing your local Internet child pornography

accurately assess document authenticity and capture both visual and electronic document data.

iDocufy works as a global KYC and AML check and enhances customer confidence due to its speed and seamless integration. When used together with BioMatch as part of our global ID, KYC & AML platform, Sodium, our solutions offer world-class authentication in one simple integration. One simple integration; a flexible 360° solution which is scalable and secure.

Utilising all forms of data, this integrated approach helps increase pass rates in countries all over the world, which in turn increases revenue and customer acquisition with real-time onboarding, creating a better customer experience.

Utilise a single element or multiple processes – it's entirely up to you. Learn more about how we can help to automate and simplify your verification processes to help you to learn more about your customers.

Book a demo today and see for yourself how powerful our suite of solutions are.

Source: [Електронний ресурс] – Режим доступу: https://hellosoda.com/blog/fakes-forgeries-and-counterfeits/https://www.quora.com/What-is-the-difference-between-forgery-and-counterfeiting

III. Post-reading activities.

Task 7. Answer the following questions.

1. What forms can identity documents take?
2. Do all countries have passports?
3. Are they unique and special?
4. What is forgery?
5. How is it punished by law in your country?
6. What is the term `counterfeit` associated with?

7. What means `to forge an object`?
8. What does forgery involve?
9. When is the world `forgery` used?
10. Why is it difficult to detect false documents?

Task 8. Complete the following sentences using the text.

1. There are thousands of _____in circulation worldwide.
2. Identity documents can take many forms – from_____, to driver's licenses, to passports and digital IDs – and it is crucial that each one is unique and has specific features that allow it to be verified.
3. Each country tends to have a list of _____identity documents that are rare, unique and protected enough to be trusted by financial institutions and when carrying out sensitive activity.
4. All countries have passports but each is _____in some way.
5. Fake, forgery and _____all mean an item is not genuine, but forgery and counterfeit implies intentional illegality.
6. Although the term counterfeit is generally _____making, dealing, or possessing any counterfeit _____, it also includes forgeries of documents and imitations of goods and trademarks.
7. To _____an object means that you fabricate by working, heating, hammering and shaping it into a certain shape.
8. Forgery could be seen as a craftsmanship, it involves_____, work and mastery and often is of quality, it's well done.
9. Usually the word forgery is used when we speak about the _____where the value is determined not by the actual document but the social or mutual agreement or culture, such as an agreement, art, or money.
10. Depending on their sophistication, _____can be difficult to detect when used to verify identity and manual identity verification checks are not just

Unit 13. Child pornography

I. <u>Pre-reading activities.</u>

Task 1. How do you understand the statement: *"Law is valuable not because it is a law, but because there is right in it"* (Beecher). **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What caused the spreading of pornography?
2. What you should do when you reveal pornographic sites?
3. What are the most common problems related to pornography?

Task 3. Try to guess the meaning of the following words.

Sexualized image, law enforcement agency, police district, child abuse, hazardous material.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. The treatment of children as <u>sexual objects</u> has existed through the ages, and so too has the production of <u>erotic literature</u> and drawings involving children.
2. Child pornography remained a <u>restricted activity</u> through most of the twentieth century.
3. The relaxation of <u>censorship standards</u> in the 1960s led to an increase in the availability of child pornography, and, by 1977, some 250 child pornography magazines were circulating in the United States, many imported from Europe.
4. An investigation that begins in one police district will almost certainly cross <u>jurisdictional boundaries</u>.

time consuming, but also produce a lengthy and clunky onboarding process for customers.

Task 9. Make a list of all the terms you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Незважаючи на те, що українські компанії активно переходять на електронний документообіг, більшість держустанов і підприємств досі використовують паперові документи. Тому ризик підробки доручень, довідок, печаток і штампів у нашій країні залишається високим. Фальшиві паспорти, дипломи, санітарні книжки, проїзні, посвідчення учасника бойових дій – це лише мала частка документів, які найчастіше підробляють в Україні. Здається, що в нас можна підробити практично все, було б бажання і, звичайно ж, гроші. А знайти виконавців подібного «замовлення» простіше простого, адже для того, щоб купити фальшиву довідку, атестат або права, досить знайти оголошення в мережі.

Як і для чого підробляють документи

Законодавство України визначає, що підробленими вважаються не тільки повністю фальшиві документи (повна підробка), але й справжні документи, в які внесені будь-які зміни, що спотворюють їх зміст (часткова підробка).

Існують також різні способи підробки документів.

Повна підробка:

1)виготовлення документа або його бланка,

2)внесення в документ неправдивих відомостей,

3)підробка підпису особи, яка засвідчує документ,

4)підробка відбитків печаток і штампів.

Task 11. Give the English equivalents of the Ukrainian words and word combinations.

Вірус, браузер, соціальна мережа, загроза, нестійкий, багатогалузевий, Троян, Мережевий хробак, шпигунські програми, файли, оперативна пам'ять, макровірус, мережа, захист комп’ютера, зломвисне програмне забезпечення, локальна мережа, операційна система, віруси-шифрувальники, користувач, пароль, обліковий запис, загроза, дискети, банківське шахрайство, антишпіонське програмне забезпечення.

Часткова підробка документів:

1)механічне видалення частини тексту,

2)видалення тексту хімічними реактивами та різними розчинниками,

3)внесення в документ нових слів, фраз або окремих знаків,

4)вклейка окремих аркушів, переклеювання фотографії, заміна аркушів.

І якщо з повністю фальшивими документами все зрозуміло, то вибір способу часткової підробки документа залежить від цілей зловмисника, який вирішив його підробити.

Підробка документів фігурує в шахрайських схемах, коли зловмисники шляхом обману хочуть незаконно й безоплатно заволодіти чужим майном. І не обов'язково мати при цьому рейдерське апетит. Шахраї зазіхають на квартири, будинки, землю й автомобілі.

Класичний приклад – купівля / продаж / оренда нерухомості. Зловмисники видають себе за реальних власників та інвесторів. Вони змінюють прізвище, ім'я, по-батькові, рік народження, або зберігають ці дані, але замінюють фотографію в паспорті.

Часто до підробки документів залучають «чорних» нотаріусів. Уповноважені нотаріуси або навіть ті, хто підробив ліцензію, пачками завіряють фальшиві документи. І, як наслідок, підставний продавець квартири надає покупцям повний пакет фальшивих документів. На вигляд не відрізнити від справжніх, адже проставлені нотаріальні печатки, а оформлення ніби відповідає букві закону.

Із продажем автомобілів така ж ситуація. Може здатися, що угода чесна та власник автомобіля «чистий». Але вже після покупки бажаного авто з'ясовується: автомобіль крадений, власник несправжній. Хоча в реєстрі жодного натяку на це.

Ухиляючись від сплати аліментів, змінюють відповідні листи в паспорті. Зокрема, на замінені чисті аркуші наносять підроблені відтиски штампів про реєстрацію, прописку та інші дані.

шкідливого ПЗ з поділом ролей і допоміжними засобами (троянські програми, завантажувачі/дропери, фішингові сайти, спам-боти і павуки).

Також розквітають соціальні технології – спам і фішинг – як засіб зараження в обхід механізмів захисту ПЗ. Спочатку на основі троянських програм, а з розвитком технологій p2p-мереж – і самостійно – набирає обертів найсучасніший вид вірусів – хробаки-ботнети (Rustock, 2006, бл. 150 тис. ботів; Conficker, 2008 – 2009, понад 7 млн ботів; Kraken, 2009, бл. 500 тис. ботів).

Віруси у складі іншого зловмисного ПЗ остаточно оформляються як засіб кіберзлочинності.

Суспільний аспект

Для одних віруси є бізнесом. Причому не тільки для їхніх авторів, але і для тих, хто з цими вірусами бореться. Бо процвітання компаній, які випускають антивірусні програми не є несподіванкою ні для кого. Для інших – це хобі. Хобі – збирання вірусних колекцій і хобі – написання вірусів. Ще інші – створюють віруси для прояву власної зухвалості і незалежності, у деяких колах подібна діяльність просто необхідна для підняття свого престижу. Є й такі, для кого віруси це витвір мистецтва; зустрічаються лікарі за покликанням, отже, може бути і комп'ютерний лікар за покликанням. Для деяких віруси служать приводом пофілософствувати на теми створення і розвитку комп'ютерного життя. Для інших віруси – це також стаття кримінального кодексу. Але для більшості користувачів комп'ютерів віруси – це щоденний головний біль і турбота, причина збоїв у роботі комп'ютера і ворог номер один.

Джерело:

https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81

заражають об'єктні файли (Shifter, 1994) і вихідні тексти програм (SrcVir, 1994).

З поширенням пакету Microsoft Office набули поширення макровіруси (Concept, 1995). У 1996 році з'явився перший вірус для Windows 95 – Win95.Boza, а в грудні того ж року – перший резидентний вірус для неї – Win95.Punch. З поширенням мереж та Інтернету файлові віруси дедалі більше орієнтуються на них як на основний канал роботи (ShareFun, 1997 – макровірус MS Word, що використовує MS-Mail для поширення, Win32.HLLP.DeTroie, 1998 — сімейство вірусів-шпигунів, Melissa, 1999 – макровірус і мережевий черв'як, який побив усі рекорди за швидкістю поширення). Еру розквіту «троянських коней» відкриває утиліта прихованого віддаленого адміністрування Back Orifice (1998) і пішли за нею аналоги (NetBus, Phase). Вірус Win95.CIH досяг апогею в застосуванні незвичайних методів, переписуючи BIOS заражених машин (епідемія в червні 1998 вважається найбільш руйнівною за попередні роки).

Наприкінці 1990-х – на початку 2000-х з ускладненням ПЗ та системного оточення, масовим переходом на порівняно захищені Windows сімейства NT, утвердженням мереж як основного каналу обміну даними, а також успіхами антивірусних технологій у виявленні вірусів, побудованих за складними алгоритмами, останні стали все більше замінювати впровадження у файли на впровадження в операційну систему (незвичайний автозапуск, руткіти) і підміняти поліморфізм величезною кількістю видів (число відомих вірусів зростає експоненціально).

Разом з тим, виявлення в Windows та іншому поширеному програмному забезпеченні численних вразливих місць відкрило дорогу черв'якам-експлоїтам. У 2004 р. безпрецедентні за масштабами епідемії викликають MSBlast (понад 16 млн систем за даними Microsoft), Sasser і Mydoom (оціночні збитки 500 млн дол. і 4 млрд дол. відповідно). Крім того, монолітні віруси значною мірою поступаються місцем комплексам

А ось підроблення статутних документів – улюблений метод рейдерів, шахраїв, які таким чином намагаються захопити певне підприємство, офіс компанії та інше майно.

Підроблюючи статутні документи, найчастіше в них вказують іншого власника, потім вносять неправдиві дані до державного реєстру юридичних осіб.

Незважаючи на те, що чи не кожен день у ЗМІ з’являється інформація про те, що поліція зловила чергову злочинну групу по підробці документів, це не зупиняє інших активно займатися подібним промислом.

Source: [Електронний ресурс] – Режим доступу: https://tsypin.partners/pidrobka-dokumentiv-shho-za-ce-zagrozhuie-i-jak-zahistitisja/

Task 11. Give the Engish equivalents of the Ukrainian words and word combinations.

Шахрайство, підробка, фальшиві документи; документи, що посвідчують особу, інтернет шахрайство, махінація, шпигунське програмне забезпечення, фальсифікація, паспорт, посвідчення водія, незаконна діяльність, фінансова установа, валюта, несанкціоноване підроблення цінних документів або предметів, електронні дані, автентичність документа.

Unit 12. Virus

I. Pre-reading activities.

Task 1. How do you understand the statement: *"After all, just one virus on a computer is one too many"*. **Translate it into Ukrainian.**

Task 2. Discuss the following questions.

1. What is a computer virus?
2. What do you understand under the term virus?
3. What computer viruses do you know?

Task 3. Try to guess the meaning of the following words.

Malware, floppy disks, vendor, peer-to-peer, legitimate-seeming, encrypt, a firewall, antispyware.

Task 4. Try to guess from the content what the underlined words and word combinations mean.

1. While free antivirus downloads are available, they just can't offer the computer virus help you need to keep up with the continuous onslaught of new strains.
2. Products like Webroot Internet Security Complete and Webroot Antivirus provide complete protection from the two most dangerous threats on the Internet – spyware and computer viruses.
3. Ransomware is a type of malware that encrypts a user's files and demands a ransom for its return.

Історія свідчить, що ідею створення комп'ютерних вірусів окреслив письменник-фантаст Т. Дж. Райн, який в одній із своїх книжок, написаній в США в 1977 р., описав епідемію, що за короткий час охопила близько 7000 комп'ютерів. Причиною епідемії став комп'ютерний вірус, який передавався від одного комп'ютера до іншого, проникав у їх операційні системи і виводив комп'ютери з-під контролю людини.

В 70-х роках, коли вийшла книжка Т.Дж. Райна, описані в ній факти здавалися фантастикою, і мало хто міг передбачати, що вже наприкінці 80-х років проблема комп'ютерних вірусів стане великою дійсністю, хоч і не смертельною для людства в боротьбі з комп'ютером, але такою, що призвела до певних соціальних і матеріальних втрат. Під час досліджень, проведених однією з американських асоціацій з боротьби з комп'ютерними вірусами, за сім місяців 1988 р. комп'ютери, які належали фірмам-членам асоціації, піддавались дії 300 масових вірусних атак, які знищили близько 300 тис. комп'ютерних систем, на відтворення яких було затрачено багато часу і матеріальних затрат. Наприкінці 1989 р. в пресі з'явилося повідомлення про знаходження в Японії нового, надзвичайно підступного і руйнівного вірусу (його назвали хробаком), за короткий час він знищив дані на великій кількості машин, під'єднаних до комунікаційних ліній. Переповзаючи від комп'ютера до комп'ютера, через з'єднувальні комунікації, «хробак» знищував вміст пам'яті, не залишаючи ніяких надій на відновлення даних.

У 1992 році з'явився перший конструктор вірусів для PC – Virus Creation Laboratory (для Amiga конструктори існували і раніше), а також готові поліморфні модулі (MtE, DAME і TPE) і модулі шифрування для вбудовування в нові віруси. У кілька наступних років було остаточно відточено стелс і поліморфні технології (SMEG.Pathogen, SMEG.Queeg, OneHalf, 1994; NightFall, Nostradamus, Nutcracker, 1995), а також випробувано самі незвичайні способи проникнення в систему і зараження файлів (Dir II – 1991, PMBS, Shadowgard, Cruncher – 1993). Крім того, з'явилися віруси, що

Жарт

Вірус-жарт Знищувач не завдає шкоди комп'ютеру, а просто лякає користувача.

Хробак

Хробак комп'ютерний Знищувач – це саморозповсюджувана програма, яка може подолати всі три етапи розповсюдження самостійно (звичайний хробак), або використовує агента-користувача тільки на 2-му етапі (поштовий черв'як).

Комбінований

Комбінований – це поєднання двох або більше типів вірусів. Назва програми «комп'ютерний вірус» походить від однойменного терміну з біології за її здатність до саморозмноження. Саме поняття «комп'ютерного вірусу» з'явилося на початку 1970-х і використовувалося у програмуванні та літературі, зокрема, у фантастичному оповіданні «Людина в рубцях» Грегорі Белфорда. Проте, автором терміну вважається Фред Коен, який у 1984 році опублікував одну з перших академічних статей, що були присвячені вірусам, де і було використано цю назву.

Для одних віруси є бізнесом. Причому не тільки для їхніх авторів, але і для тих, хто з цими вірусами бореться. Бо процвітання компаній, які випускають антивірусні програми не є несподіванкою ні для кого. Для інших – це хобі. Хобі – збирання вірусних колекцій і хобі – написання вірусів. Ще інші – створюють віруси для прояву власної зухвалості і незалежності, у деяких колах подібна діяльність просто необхідна для підняття свого престижу. Є й такі, для кого віруси це витвір мистецтва; зустрічаються лікарі за покликанням, отже, може бути і комп'ютерний лікар за покликанням. Для деяких віруси служать приводом пофілософствувати на теми створення і розвитку комп'ютерного життя. Для інших віруси – це також стаття кримінального кодексу. Але для більшості користувачів комп'ютерів віруси – це щоденний головний біль і турбота, причина збоїв у роботі комп'ютера і ворог номер один.

4. When a device does become infected, though, installing an antivirus solution is still your best bet for removing it.

5. Most, but not all, computer viruses require a user to take some form of action, like enabling “macros” or clicking a link, to spread.

Task 5. Match the English phrases on the left with their Ukrainian equivalents on the right.

1. malicious	a) безперестанку
2. malware	b) постачальники
3. relentlessly	c) шахрайство
4. sapping	d) шкідливе програмне забезпечення
5. vulnerable	e) зловмисний
6. fraud	f) підривати
7. vendors	g) вразливий

II. While-reading activities.

Task 6. Read the text and answer the questions. Translate the text into Ukrainian.

1. What does a computer virus do?
2. What are the symptoms of a computer virus?
3. How can you protect your computer?

Virus

What is a computer virus?

A computer virus is a malicious piece of computer code designed to spread from device to device. A subset of malware, these self-copying threats are usually designed to damage a device or steal data.

Think of a biological virus – the kind that makes you sick. It's persistently nasty, keeps you from functioning normally, and often requires something powerful to get rid of it. A computer virus is very similar. Designed to replicate relentlessly, computer viruses infect your programs and files, alter the way your computer operates or stop it from working altogether.

What does a computer virus do?

Some computer viruses are programmed to harm your computer by damaging programs, deleting files, or reformatting the hard drive. Others simply replicate themselves or flood a network with traffic, making it impossible to perform any internet activity. Even less harmful computer viruses can significantly disrupt your system's performance, sapping computer memory and causing frequent computer crashes.

How do computer viruses spread?

Viruses can be spread several ways, including via networks, discs, email attachments or external storage devices like USB sticks. Since connections between devices were once far more limited than today, early computer viruses were commonly spread through infected floppy disks.

Today, links between internet-enabled devices are for common, providing ample opportunities for viruses to spread. According to the U.S. Cybersecurity and Infrastructure Security Agency, infected email attachments are the most common means of circulating computer viruses. Most, but not all, computer viruses require a user to take some form of action, like enabling "macros" or clicking a link, to spread.

What are the symptoms of a computer virus?

Your computer may be infected if you recognize any of these malware symptoms:

- Slow computer performance

За створення та поширення шкідливих програм (в тому числі вірусів) у багатьох країнах передбачена кримінальна відповідальність. Зокрема, в Україні поширення комп'ютерних вірусів переслідується і карається відповідно до Кримінального кодексу (статті 361, 362, 363).

Комп'ютерні віруси бувають п'яти типів:

- Шкідник
- Знищувач
- Хробак
- Жарт
- Комбінований
- Шкідник

Вірус шкідник – робить якусь шкоду користувачу, аби роздратувати.

Вірус шкідник може зробити наступні дії:

- Перемістити вказівник миші на протилежну сторону від справжньої
- Вимкнути мишу
- Вимкнути клавіатуру
- Заборонити постачання відео сигналу
- Відкривати програму без команди користувача
- Відкривати вкладку у браузері без команди користувача

Вірус, який знищує:

- Системні файли
- Документи
- Утиліти
- Ігри
- Відеозаписи
- Музику
- Фотографії
- Драйвери

9. They prevent viruses from entering your computer, stand guard at every possible _____ of your computer and fend off any computer virus that tries to open, even the most damaging and devious strains.

10. Previously undetected forms of polymorphic malware can often do the most damage, so it's critical to have _____, guaranteed antivirus protection.

Task 9. Make a list of all the terms/procedures/experiments/pieces of equipment you can find in the text. Check all the examples in pairs. What are they used for? Discuss them in pairs. Give their Ukrainian equivalents.

Task 10. Translate from Ukrainian into English.

Комп'ютерний вірус (англ. computer virus) – комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макровіруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу.

Розробники вірусного програмного забезпечення використовують засоби соціальної інженерії і інформацію про вразливості цільового ПЗ, щоб заражувати системи і розповсюджувати вірус. Необізнані користувачі ПК помилково відносять до комп'ютерних вірусів також інші види зловмисного ПЗ – програм-шпигунів чи навіть спам.

Кожного року комп'ютерні віруси причиняють шкоди розміром в декілька мільярдів доларів, викликаючи системні критичні помилки, зупиняючи великі сайти та вебдодатки, знищуючи або модифікуючи файли, підвищуючи час відклику[1].

- Erratic computer behavior
- Unexplained data loss
- Frequent computer crashes

How are computer viruses removed?

Antiviruses have made great progress in being able to identify and prevent the spread of computer viruses. When a device does become infected, though, installing an antivirus solution is still your best bet for removing it. Once installed, most software will conduct a "scan" for the malicious program. Once located, the antivirus will present options for its removal. If this is not something that can be done automatically, some security vendors offer a technician's assistance in removing the virus free of charge.

Examples of computer viruses

In 2013, the botnet virus Gameover ZueS was discovered to use peer-to-peer downloading sites to distribute ransomware and commit banking fraud. While tens of thousands of computer viruses still roam the internet, they have diversified their methods and are now joined by several malware variants like:

- Worms - A worm is a type of virus that, unlike traditional viruses, usually does not require the action of a user to spread from device to device.

Trojans - As in the myth, a Trojan is a virus that hides within a legitimate-seeming program to spread itself across networks or devices.

Ransomware - Ransomware is a type of malware that encrypts a user's files and demands a ransom for its return. Ransomware can be, but isn't necessarily, spread through computer viruses.

Computer virus protection

When you arm yourself with information and resources, you're wiser about computer security threats and less vulnerable to threat tactics. Take these steps to safeguard your PC with the best computer virus protection:

- Use antivirus protection and a firewall
- Get antispyware software
- Always keep your antivirus protection and antispyware software up-to-date

- Update your operating system regularly
- Increase your browser security settings
- Avoid questionable Websites
- Only download software from sites you trust.
- Carefully evaluate free software and file-sharing applications before downloading them.
- Don't open messages from unknown senders
- Immediately delete messages you suspect to be spam

An unprotected computer is like an open door for computer viruses. Firewalls monitor Internet traffic in and out of your computer and hide your PC from online scammers looking for easy targets. Products like Webroot Internet Security Complete and Webroot Antivirus provide complete protection from the two most dangerous threats on the Internet – spyware and computer viruses. They prevent viruses from entering your computer, stand guard at every possible entrance of your computer and fend off any computer virus that tries to open, even the most damaging and devious strains.

While free antivirus downloads are available, they just can't offer the computer virus help you need to keep up with the continuous onslaught of new strains. Previously undetected forms of polymorphic malware can often do the most damage, so it's critical to have up-to-the-minute, guaranteed antivirus protection.

Джерело: https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses

III. Post-reading activities.

Task 7. Answer the following questions.

1. How are computer viruses spread?

2. How does one protect my computer from a virus?

3. Howis the virus infection removed?

4. What do hackers use computer viruses for?

5. What does one do if finds a virus on a computer?

6. What should I do when I receive a potentially virus infected message?

7. What is the difference between a virus and malware?

8. How does an antivirus work?

9. Can a virus damage computer hardware?

10. What is computer security?

Task 8. Complete the following sentences using the text.

1. A subset of malware, these self-copying threats are usually _____ to damage a device or steal data.

2. Designed to replicate _____, computer viruses infect your programs and files, alter the way your computer operates or stop it from working altogether.

3. Some computer viruses are programmed _____ your computer by damaging programs, deleting files, or reformatting the hard drive.

4. Since _____ between devices were once far more limited than today, early computer viruses were commonly spread through infected floppy disks.

5. Most, but not all, computer viruses require a user to take some form of action, like _____ "macros" or clicking a link, to spread.

6. When a device does become infected, though, installing an antivirus _____ is still your best bet for removing it.

7. In 2013, the botnet virus Gameover ZueS was discovered to use _____ downloading sites to distribute ransomware and commit banking fraud.

8. When you arm yourself with information and resources, you're wiser about computer security threats and less _____ to threat tactics.