СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации / Ю. Н. Загинайлов – Барнаул: Изд-во АлтГТУ, 2010. – 104 с.
2. Информационная безопасность человека – [Електронний ресурс], режим доступу: https://www.mindmeister.com/ru/981251359/_ – березень 2018.
3. Информационная безопасность предприятия: ключевые угрозы и средства защиты – [Електронний ресурс], режим доступу: https://www.kp.ru/guide/informatsionnaja-bezopasnostpredprijatija.html – березень 2018.
4. Інформаційна безпека України – [Електронний ресурс], режим доступу: http://pidruchniki.com/18340719/politologiya/informatsiyna_bezpeka_ukrayini – березень 2018.

Сембрат Дем'ян Сергійович, ст. гр. 2АВ-14б, факультету комп'ютерних систем та автоматики Вінницького національного технічного університету, м. Вінниця , e-mail: sdsvin@gmail.com.

Sembrat Demian, 2AV-14b of the group, Faculty of Computer Systems and Automation, Vinnytsia national technical university, Vinnytsia, mail: sdsvin@gmail.com.

УДК 61.4

М. В. Петричко
І. В. Віштак

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗГІДНО ЗАКОНОДАВСТВА ЄС

Вінницький національний технічний університет

Запропоновано заходи стосовно швидкого реагування на існуючі виклики інформаційної безпеки. Подано напрямки діяльності політики ЄС стосовно інформаційної безпеки. Визначено дії, що порушують безпеку інформаційних мереж і систем.

Ключові слова: інформаційна безпека, ЄС, кібербезпека.

PROVIDING INFORMATION SECURITY ACCORDING TO EU LEGISLATION

Proposed ways of fast reacting on existed information security leaks. Given EU's activities politics directions for information security. Defined actions violating information network's and systems's security.

Keywords: informational security, EU, cyber security.

Важливими напрямками сучасного етапу розвитку людства є посилення міждержавних інформаційних потоків, поширення різноманітних способів і засобів інформаційного обміну, що практично не контролюються державою. За цих умов набувають поширення нові – інформаційні – загрози та виклики, що вимагають від держав негайного реагування й застосування нестандартних заходів і рішень. У зв'язку з цим на різних рівнях комунікації постає питання інформаційної безпеки. Активну політику в сфері інформаційної безпеки проводить Європейський Союз.

Результати дослідження

У зв'язку з автоматизацією процесів виробництва та управління, розвитком обчислювальної техніки значного розповсюдження набули професії в яких комп'ютер використовується як основний засіб праці [1, 2].

У 2001 році Європейською Комісією було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід» (Network and Information

Security: Proposal for A European Policy Approach), в якому окреслено європейський підхід до проблеми інформаційної безпеки. У документі використовується термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, аутентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [3].

Дії, що порушують безпеку інформаційних мереж і систем, згруповані таким чином:

- перехоплення електронної комунікації, копіювання або модифікація даних;
- неавторизований доступ до комп'ютера або комп'ютерних мереж;
- деструктивні атаки на мережі, зокрема атаки на доменні імена, перевантаження мережі штучними повідомленнями, атаки, спрямовані на порушення маршрутизації;
- шкідливе програмне забезпечення;
- підробка веб-сайтів;
- без пекові інциденти як наслідок непередбачених і ненавмисних подій, таких як природні катаклізми, збої у роботі апаратних засобів та програмного забезпечення, людські помилки.

У документі визначено такі основні напрями європейської політики інформаційної безпеки:

1. Підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами.
2. Створення європейської системи попередження та інформування про нові загрози
3. Забезпечення технологічної підтримки
4. Підтримка ринково орієнтованої стандартизації та сертифікації
5. Правове забезпечення
6. Зміцнення безпеки на державному рівні
7. Розвиток міжнародного співробітництва з питань інформаційної безпеки.

10 березня 2004 року було створено Європейську агенцію з питань мережевої та інформаційної безпеки (European Network and Information Security Agency - ENISA). Це спеціалізована агенція ЄС, діяльність якої спрямована на зміцнення можливостей європейської спільноти, країн-членів, а також ділових кіл в сфері попередження і реагування на проблеми, пов'язані з інформаційною безпекою.

Основними напрямами діяльності Агенції є: надання консультацій та допомоги Комісії і країнам-членам в сфері інформаційної безпеки; збір та аналіз даних щодо безпекових інцидентів в Європі та ризиків, що виникають; розробка методів оцінки та управління ризиками для підвищення здатності ЄС реагувати на загрози інформаційній безпеці; підвищення обізнаності та розвиток співробітництва між різними акторами в сфері інформаційної безпеки, зокрема шляхом стимулювання взаємодії між державним і приватним секторами. Агенція також допомогає Європейській Комісії у попередній технічній роботі з метою оновлення і вдосконалення європейського законодавства в сфері мережевої та інформаційної безпеки [3].

Для ефективного реагування ЄС на існуючі виклики кібербезпеці необхідна реалізація заходів:

1. Забезпечення належного рівня підготовки на всіх рівнях, що передбачає визначення країнами-членами базових можливостей для національних Комп'ютерних команд швидкого реагування та систем реагування на безпекові інциденти;
2. Створення європейської системи раннього сповіщення про кіберзагрози;
3. Зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС, що передбачає розробку національних планів реагування на надзвичайні події та організація тренінгів для широкомасштабного реагування на безпекові інциденти; проведення панєвропейських навчань з проблеми безпекових інцидентів в мережі Інтернет; зміцнення співпраці між національними комп'ютерними групами швидкого реагування;
4. Вироблення європейських керівних принципів щодо забезпечення стійкості і стабільності мережі Інтернет та їхнє просування на міжнародній арені;
5. Визначення критеріїв ідентифікації європейської критичної інфраструктури для сектору інформаційно-комунікаційних технологій.

Висновки

Таким чином, в рамках ЄС інформаційна безпека розглядається, насамперед, як такий стан інформаційних мереж і систем, що забезпечує достатній рівень захисту цілісності, доступності й приватності інформації. Відповідно одним з пріоритетів політики країн ЄС в сфері інформаційної

безпеки є розробка і впровадження програм та різних технічних засобів, які дозволяють підтримувати певний рівень захисту інформаційно-комунікаційних технологій. Іншим пріоритетом політики ЄС є інформаційна безпека громадян.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Дембіцька С. В. Умови попередження стресу в професійній діяльності системного інженера / С. В. Дембіцька – [Електронний ресурс], режим доступу: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/11074/478.pdf?sequence=3.

2. Віштак І. В. Особливості формуваннння культури безпеки в процесі підготовки фахівців технічних спеціальностей / І. В. Віштак // Педагогіка безпеки. - Вінниця : ВНТУ, 2016. - № 1. - С. 32-39.

3. Communication from the European Commission: "Network and Information Security: Proposal for a European Policy Approach" (COM (2001) 298 (June 6, 2001) - http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf

4. The European Network and Information Security Agency (ENISA). - http://www.enisa.europa.eu/.

Микола Володимирович Петричко – студент групи 1АВ-14б, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця, e-mail: petrychko.myckola@gmail.com
Віштак Інна Вікторівна – кандидат технічних наук, доцент, доцент кафедри Безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, Вінниця, e-mail: innavish322@gmail.com.

Petrychko Mykola V. – student of the group 1AV-14b, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: petrychko.myckola@gmail.com
Vishtak Inna V. – Cand. Sc. (Eng.), Assistant Professor, Assistant Professor of Department of Health and Safety Studies, Vinnitsa National Technical University, e-mail: innavish322@gmail.com

УДК 621.373.826

О. О. Плешко
І. В. Віштак

БЕЗПЕКА ПРИ РОБОТІ З БІОЛОГІЧНИМИ ФАКТОРАМИ

Вінницький національний технічний університет

В статті розглянуто вимоги безпеки при роботі з біологічними факторами.. Наводиться перелік біологічних чинників, які створюють значні проблеми для забезпечення нормальної життєдіяльності людини, а також бактеріальна забрудненість на прикладі молочної продукції.
Ключові слова: біологічні фактори, мікроорганізми, мікробіологічні фактори, фактори ризику.

SAFETY IN BUSINESS WITH BIOLOGICAL FACTORS

The article considers the safety requirements when working with biological factors. The list of biological factors that create significant problems for ensuring normal human life, as well as bacterial contamination on the example of dairy products is given.
Keywords: biological factors, microorganisms, microbiological factors, risk factors.

Біологічні чинники природного походження створюють значні проблеми для забезпечення нормальної життєдіяльності людини. Крім цього, певні соціальні умови теж сприяють виникненню та поширенню окремих видів захворювань. Усе це становить так звану природно-соціальну небезпеку.

Одним із видів небезпеки людини у соціальному середовищі є біологічні структури, до яких відносять макроорганізми (рослини і тварини) і патогенні мікроорганізми, збудники інфекційних захворювань (бактерії, гриби, віруси, спірохети, найпростіші).

Продукти харчування, що споживаються щодня кожною людиною, повинні грати роль не