професійних користувачів протягом робочої зміни повинні встановлюватися регламентовані перерви. Тривалість безперервної роботи з приладом без регламентованої перерви не повинна перевищувати 2 години. Під час регламентованих перерв з метою зниження нервово-емоційного напруження, зорового і загального стомлення доцільно виконувати комплекси вправ, рекомендованих санітарними нормами і правилами. Особам, які працюють з приладами для дилатометричних досліджень з високим рівнем напруженості праці під час регламентованих перерв і в кінці робочого дня рекомендовано психологічне розвантаження у спеціально обладнаних приміщеннях.

Після закінчення роботи необхідно знеструмити всі джерела обчислювальної техніки і периферійне обладнання.

Вимоги безпеки з приладом в аварійних ситуаціях

При виникненні аварійної ситуації на робочому місці особа, що працює з приладом зобов'язана роботу припинити, вимкнути електроенергію, повідомити керівника і вжити заходів до ліквідації цієї ситуації.

У разі виникнення пожежі вимкнути прилад з електромережі, викликати пожежну охорону і приступити до гасіння пожежі наявними засобами пожежогасіння.

При наявності травмованих усунути вплив факторів, що загрожують здоров'ю та життю постраждалих (звільнити від дії електричного струму, погасити палаючий одяг і т.д.), надати першу допомогу, викликати швидку медичну допомогу або лікаря або вжити заходів для транспортування потерпілого до найближчої медичної установи , повідомити про те, що трапилося керівнику[2-4].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Компан Т. А. Измерительные возможности и перспективы развития дилатометрии [Електронний ресурс] // Режим доступу: http://www.ria-stk.ru/mi/adetail.php?ID=51505 (дата звернення 13.03.2018).
2. [Електронний ресурс] // Режим доступу: http://vsegost.com/Catalog/57/574.shtml (дата звернення
3. 13.03.2018).
4. [Електронний ресурс] // Режим доступу: https://dnaop.com/html/43076/doc-ДНАОП_4559-88 (дата звернення 13.03.2018).
5. [Електронний ресурс] // Режим доступу http://www.know-house.ru/gost/sp_2013/sp_44.13330.2011.pdf

Каращенко Марія Ігорівна: студентка групи МІТ-14б факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця.

Maria Karashchenko: student of the group MIT-14b, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnitsa.

УДК 334.72

Д. С. Сембрат

НАСЛІДКИ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вінницький національний технічний університет

В даній статті розглянуто основні види загроз та наслідки вразливості інформаційної безпеки, їх вплив на підприємства, людей та державу.

Ключові слова: інформаційна безпека, вразливість, загрози.

EFFECTS OF INFORMATION SECURITY VULNERABILITY

The article deals with the main types of threats and effects of information security vulnerability, their impact on enterprises, peoples and state.

Keywords: information security, vulnerability, threats.

Під інформаційною безпекою розуміється захищеність інформації від дій, які призводять до нанесення шкоди її власникам чи користувачам. Такі дії можуть бути як і випадковими, так і навмисними. Саме тому, інформаційна безпека повинна бути спрямованою на запобігання ризиків, а не на усунення наслідків.

Вразливість інформаційної безпеки – нездатність системи протистояти подіям або діям, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [1].

Очевидно, що порушення інформаційної безпеки може призвести до нанесення збитків. Вразливість інформаційної безпеки загрожує не лише компаніям, підприємствам, державним установам, а і людям. Такі загрози поділяються на 3 види [2]:

загрози конфіденційності (неправомірний доступ до інформації);

загрози доступності (здійснення дій, що унеможливлюють чи затрудняють доступ до ресурсів інформаційної системи);

загрози цілісності (неправомірна зміна даних).

Найчастіше з компаній «витікають» конфіденційні дані: інформація фінансового характеру, що може призвести до великих матеріальних втрат, або ж персональні дані співробітників, що порушує конфіденційність, оскільки все, що стосується діяльності компанії, має залишатися всередині компанії і повинно бути захищеним від загроз [3].

Шахрайство – одна із основних загроз доступності в інформаційній безпеці. До такого виду шахрайства відносять маніпуляції з платіжними картками та здійснення несанкціонованого доступу до онлайн-банків. Метою цих економічних злочинів є обхід законодавства, політики або ж привласнення майна.

Втрата даних чи порушення цілісності інформації можуть бути викликаними несправністю обладнання або навмисними діями користувачів (співробітниками компаній або зловмисниками). Порушення цілісності інформації, наприклад, у політичній сфері держави, може призвести не лише до проблем, пов’язаних з конфіденційністю, а й до антропогенних небезпек соціального характеру (бунтів, страйків, протестів), що може нести прямий вплив на здоров’я людини.

Окрім загроз, напряму пов’язаних з інформаційною безпекою, варто розуміти, що інформаційна безпека є органічною складовою національної безпеки. Процес інформування суспільства розвивається стрімко та часто є непередбачуваним, що призводить до створення єдиного інформаційного простору, в межах якого суб’єкти цього ж простору (окремі особи, організації, підприємства) зберігають, накопичують інформацію та обмінюються нею.

Якість функціонування та безпека інформаційного середовища, рівень розвитку та рівень і стан нормативно-правового забезпечення даних процесів визначають нормальну життєдіяльність суспільства. На закріплення державної інформаційної політики спрямоване інформаційне законодавство. Це передбачає забезпечення якісного рівня національної безпеки в інформаційній сфері, нормальний розвиток інформаційних технологій і засобів гарантованого захисту інформації.

Усі сфери діяльності (виробництво, органи управління та оборони, зв'язок та транспорт, банківська справа, наука й освіта, медицина) все більше залежать від інтенсивності інформаційного обміну, повноти, своєчасності та достовірності інформації. З того часу як з’явились та широко активізувалися загрози в інформаційній сфері, перш за все загрози від ведення інформаційних війн, суттєво підвищилася роль і значення інформаційної безпеки в системі національної безпеки України [4].

Розглядаючи наслідки вразливості інформаційної безпеки, необхідно розуміти, що вплив, який може отримати людина через проблеми чи відсутність інформаційної безпеки, може нести загрозу не лише матеріального чи морального характеру, а й фізичного та психологічного, що порушує безпеку життєдіяльності.

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