law enforcement agencies and central and local executive authorities in this area. A rather good example to follow is Estonia, which has succeeded because of modern innovations that Ukraine lacks to overcome crimes against curatorship.

Список використаних джерел:

1. Buhaichuk, K., Sviatokum, I., Chumak, V. (2016). Zakordonnyi dosvid otsinky efektyvnosti politseiskoi diialnosti ta perspektyvy yoho vykorystannia v Ukraini [Foreign experience in evaluating the effectiveness of police activities and the prospects for its use in Ukraine] (Scientific and methodological recommendations). Kharkiv: Kharkiv National University of Internal Affairs. [in Ukrainian]. – Режим доступу: http://pbz.nlu.edu.ua/article/viewFile/157068/156376

2. Knoema [Електронний ресурс]. – Режим доступу: http://knoema.ru/atlas/ Япония/topics/Преступность. – Заголовок з екрану. – Режим доступу: http://dspace.nlu.edu.ua/bitstream/123456789/11144/1/Kolodygnuy_74-75.pdf

3. Белявская О. А. Уголовная политика в Японии / О. А. Белявская // Актуальные вопросы борьбы с преступностью в России и за рубежом. – М., 1992. – Вып. 7. – 56 с.

4. Wood A. Japan May Offer A Way Forward For Better Community Policing in Bibb County / A.Wood [Електронний ресурс]. – Режим доступу: http://maconmonitor.com/2015/03/26/japanese-kobans-community-policing/. –

5. EGOV – усі сервіси України.URL: https://egov.in.ua/

Робейко О.,
здобувач ступеня вищої освіти бакалавра
Національної академії
внутрішніх справ
Консультант з мови: Грицук Л.

USA-ERFAHRUNG IN DER INFORMATIONSSICHERHEIT UND DER BEKÄMPFUNG VON CYBERKRIMINALITÄT

Heutzutage ist Datenschutz kein Privileg, sondern eine Notwendigkeit. Sie betrifft nicht nur die Strukturen, deren Risiken im Laufe ihrer Aktivitäten erhöht werden, wie z.B. IT-Unternehmen, sondern auch die Gesellschaft und die Staaten. Bei der Bestellung der Entwicklung eines bestimmten Produkts müssen alle sicher sein, dass es keine Möglichkeit für

Datenverlust besteht, dementsprechend, dass es Sicherheit der Informationen gibt, die dem Entwickler zur Verfügung gestellt werden [1].

Als Informationssicherheit bezeichnet man Eigenschaften von technischen oder nicht-technischen Systemen zur Informationsverarbeitung, -speicherung und -lagerung, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken [2].

In der Praxis orientiert sich die Informationssicherheit im Rahmen des IT-Sicherheitsmanagements unter anderem an der internationalen ISO/IEC-27000-Reihe. Im deutschsprachigen Raum ist ein Vorgehen nach IT-Grundschutz verbreitet. Im Bereich der Evaluierung und Zertifizierung von IT-Produkten und -systemen findet die Norm ISO/IEC 15408 häufig Anwendung [3].

Die Gesetze zur IT-Sicherheit, Informationssicherheit und Datenschutz in den USA sind relativ flexibel und im Vergleich weniger streng gehalten. Sie sind aus hundert Jahren Erfahrung mit Datenschutz- und Strafrechtsnormen erwachsen und haben sehr wenig mit dem Schutz der Vertraulichkeit und der Integrität von Systemen, Personen, Netzwerken und Daten zu tun. Die Normen wurden im Laufe der Zeit überarbeitet, um den heutigen Anforderungen an die IT-Sicherheit und den Datenschutz gerecht zu werden. Außerdem hängt die Verordnung von Datenschutzgesetzen stark von staatlichen Reaktionen auf Vorfälle und private Klagen gegen Unternehmen ab. Dieses Konstrukt des US-amerikanischen Rechtssystems führt dazu, dass die Gesetzeslage zur IT-Sicherheit und zum Datenschutz nur als ein „Framework“ von Regeln und Vorschriften betrachtet wird, welches keinen zuverlässigen Schutz der Privatsphäre gewährleistet [4].

In der Regel führen Verstöße gegen Bundes- und Bundesstaats-Datenschutzgesetze zu zivil-, aber nicht strafrechtlichen Strafen. Das Gesetz sieht vor, dass Privatpersonen Unternehmen vor Gericht ziehen dürfen, wenn sie der Meinung sind, dass ein Unternehmen gegen die Gesetze verstoßen hat. Cyberkriminalität in den USA umfasst Phishing, Hacking, Identitätsbetrug, elektronischer Diebstahl, der Besitz von Hard- und Software für cyberkriminale Aktivitäten, die Infizierung von IT-Systemen mit Malware und Ransomware sowie Kinderpornographie (nach dem Computer Fraud and Abuse Act von 1986). Straftäter bekommen eine Strafe von bis zu 20 Jahren Gefängnis und/oder eine Geldstrafe, je nach Art und Schwere der Straftat [5].

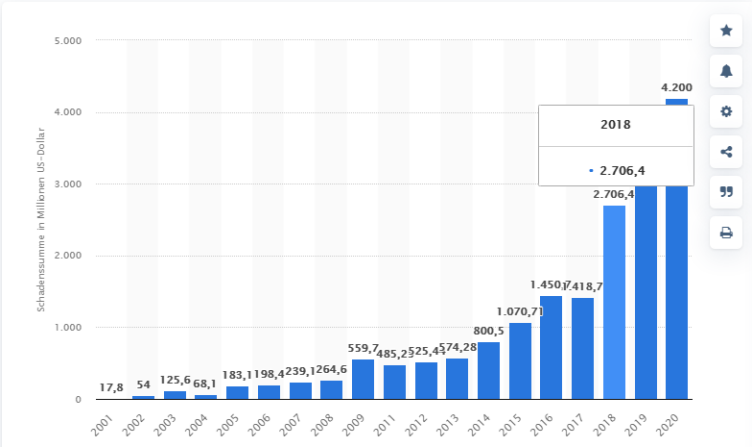
Für die meisten Fälle von Cyberkriminalität sind Cyberkriminelle oder Hacker verantwortlich. Deren Ziel ist es, auf diese Art an Geld zu kommen.

Cyberkriminalität geht sowohl von Einzelpersonen als auch von Organisationen aus [6].

Internetkriminalität oder Cyberkriminalität tritt in verschiedenen Formen in Erscheinung. Nach einer Definition des Bundeskriminalamtes umfasst Internetkriminalität (im engeren Sinne) alle „Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten“.

Eine dieser Formen von Internetkriminalität ist Phishing. Der Begriff Phishing setzt sich laut dem Bundesamt für Sicherheit in der Informationstechnik aus den Wörtern "Password" und "fishing" zusammen und benennt das Vorgehen, illegal Daten von Internetnutzern über gefälschte Webseiten, E-Mails oder Kurznachrichten zu beschaffen, um damit einen Identitätsdiebstahl zu begehen. Ziel dieser Form der Internetkriminalität sind die vertraulichen Daten des Nutzers, wie z.B. Passwörter, Kreditkartennummern oder Kontodaten, um mit den erhaltenen Daten beispielsweise Kontoplünderungen zu begehen. Im März 2020 belief sich die Anzahl der entdeckten Phishing-Webseiten auf rund 60.300. Optisch fällt es schwer, gefälschte Internetseiten von ihren echten Vorbildern zu unterscheiden. Auch inhaltlich wirken die sogenannten Phishing-Seiten mittlerweile seriös und vertrauenswürdig [7].

Schadenssumme durch angezeigte Internetkriminalität in den USA in den Jahren 2001 bis 2020 (in Millionen US-Dollar)



Zu den offiziellen Dokumenten zu Aspekten der Informationssicherheit gehören der Bericht des US-Verteidigungsministeriums "Report of the Guardrennial Defense Review", das Konzeptdokument der Joint Chiefs of Staff "Joint Vision 2010", der Bericht der Nationalen Verteidigungskommission "Transformation of

National Security Defense in the 21st Century, Report of the National Defense Council". Sie stellen fest, dass der Staat nicht in der Lage ist, die Probleme, die in der Welt auftreten können, vorherzusehen und zu vermeiden. Sie glauben, dass die Strategie zuerst die Streitkräfte ist, um diese Probleme zu bewältigen [8].

Also, der Zustand und aktuelle Trends der US-Informationssicherheit und der Entwicklung der Cyberkriminalität werden analysiert. Man kann darauf hingewiesen, dass die US-Informationssicherheit eine der Hauptkomponenten der nationalen Sicherheit ist. Die USA schenkt dieser Frage große Aufmerksamkeit, vielleicht deshalb war und bleibt der Staat als einer der führenden Staaten der Welt in verschiedenen Bereichen: politischen, wirtschaftlichen, militärischen u.a.

Список використаних джерел:

1. http://www.irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Chkup_2011_1_81.pdf

2. Stefan Loubichi: *IEC 62443: IT-Sicherheit für industrielle Automatisierungssysteme – eine Einführung in die Systematik* VGB PowerTech Journal, Ausgabe 6/2019, ISSN 1435-3199

3. https://de.wikipedia.org/wiki/Informationssicherheit

4. https://digitaleweltmagazin.de/2019/05/27/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/

5. https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ccmanual.pdf

6. https://www.kaspersky.de/resource-center/threats/what-is-cybercrime

7. https://de.statista.com/themen/1834/internetkriminalitaet/#dossierKeyfigures

8. http://conf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iv-konferentsii-2016-g/112-sobko