Н. Ж. Апахаев, И. Т. Мусабекова,
И. С. Амреева

КИБЕРПРЕСТУПНОСТЬ

УЧЕБНОЕ ПОСОБИЕ

Н.Ж. Апахаев, И.Т. Мусабекова, И.С. Амреева

КИБЕРПРЕСТУПНОСТЬ

Учебное пособие

Алматы 2022

УДК 343 (075.д)
ББК 67.408я73

Рассмотрено и одобрено на заседании методического совета Академии «Кайнар». Протокол № 5/76 от 27 декабря 2021 года.

Рецензенты:
Алмагамбетов П.А.;
Тлеуов Г.Б.

Н.Ж. Апахаев, И.Т. Мусабекова, И.С. Амреева.
Киберпреступность: учебное пособие (конспект лекций)

ISBN 978-601-08-1404-2

Данная работа представляет собой учебное пособие, в которой с раскрываются общие теоретические аспекты киберпреступности.

Пособие рассчитано на студентов, преподавателей высших учебных заведений, сотрудников правоохранительных органов.

УДК 343 (075.д)
ББК 67.408я73

ISBN 978-601-08-1404-2

ОГЛАВЛЕНИЕ

Введение

Информационно-коммуникационные технологии (ИКТ) изменили способы, при помощи которых люди ведут свои дела, покупают товары и услуги, отправляют и получают деньги, общаются, обмениваются информацией, взаимодействуют друг с другом, формируют и развивают отношения с другими людьми. Такие изменения, а также постоянно растущие масштабы использования ИКТ и зависимость от них создают уязвимости, которыми могут воспользоваться преступники и другие злоумышленники, нацеленные на ИКТ и/или использующие ИКТ для совершения преступлений. В данном учебном пособии дается представление об основных понятиях, относящихся к киберпреступности, рассказывается о том, что такое киберпреступность, рассматриваются тенденции в области развития Интернета, технологий и киберпреступности, а также проблемы технического, правового, этического и оперативного характера, связанные с расследованием киберпреступлений и предупреждением киберпреступности. В литературе для чтения, выбранной для данного предмета, содержится обзор ключевых понятий, основных терминов и определений, а также общие сведения о киберпреступности, связанных с ней проблемах и мерах по ее предупреждению.

Тема 1. Введение в киберпреступность.

1. Основы компьютерных технологий.

Компьютерная система может быть представлена настольными или портативными компьютерами. Однако мобильные телефоны, планшетные компьютеры и устройства Интернета вещей (IoT), являющиеся устройствами, подключенными к Интернету (например, бытовые приборы и умные часы), которые взаимосвязаны и взаимодействуют друг с другом и позволяют отслеживать объекты, людей, животных и/или растения, а также обмениваться информацией о них с целью предоставления пользователям этих устройств определенной услуги, а также многие другие устройства также могут рассматриваться в качестве компьютерных систем.

Существуют разные определения компьютерной системы. Например, статья 1(a) Конвенции Совета Европы о киберпреступности 2001 года определяет «компьютерную систему» как «любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных» (для ознакомления с руководящими указаниями в отношении толкования понятия «компьютерная система», включенного в Конвенцию, см. публикацию Комитета участников Конвенции о киберпреступности 2012 года (Cybercrime Convention Committee, 2012). В то же время в статье 1 Конвенции Африканского союза о кибербезопасности и защите персональных данных 2014 года компьютерная система определяется как «электронное, магнитное, оптическое, электрохимическое или иное высокоскоростное устройство обработки данных или группа взаимосвязанных или сопряженных устройств, выполняющих логические, арифметические функции или функции хранения, включая средство хранения данных или средство связи, непосредственно связанное с таким устройством или такими устройствами или работающее в сочетании с таким устройством или такими устройствами».

Компьютерные системы имеют свойство обрабатывать данные. Статья 2(3) Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года определяет данные как «все, что может храниться, обрабатываться, генерироваться и передаваться с помощью информационных технологий, например, цифры, буквы, символы и т.д.». Для обозначения данных используются и другие термины: в статье 1 (b) Конвенции Совета Европы о киберпреступности используется термин «компьютерные данные» («любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программу, подходящую для того, чтобы компьютерная система выполняла функцию»; в статье Конвенции Африканского союза о кибербезопасности и защите персональных данных 2014 года используется термин «компьютеризированные данные», который имеет практически такое же определение данных, что и термин, используемый в Конвенции Совета Европы о киберпреступности 2001 года («любое представление фактов, информации или понятий в форме, подходящей для обработки в

/https://caselaw.findlaw.com/us-2nd-circuit/1862572.html
54. Newman, 2018./https://global.oup.com/academic/product/networks-9780198805090?cc=us&lang=en&#
55. Morgan, 2018. /https://www.jpmorgan.com/solutions/cib/insights/health-care-conference
56. Alvarez, Hall, and Hyde, 2008 /https://www.jstor.org/stable/41403728
57. McGuire and Dowling, 2013. /https://assets.publishing.service.gov.uk/government/ uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
58. Europol, 2018./ https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2018.
59. Read et al., 2016. /https://agupubs.onlinelibrary.wiley.com /doi/10.1002/2016WR019993
60. Conrad, Dorn, and Craiger, 2010. /https://commons.erau.edu/publication/999/
61. Casey, Ferraro, and Nguyen, 2009. /https://www.researchgate.net/ publication/26819089_Investigation_Delayed_Is_Justice_Denied_Proposals_for_Expediting_Forensic_Examinations_of_Digital_Evidence.
62. Tcherni et al., 2016./https://www.researchgate.net/publication/305630752_ Reasons_for_Gaps_in_Crime_Reporting_The_Case_of_White-Collar_Criminals_Investigated_by_Private_Fraud_Examiners_in_Norway
63. Smeets, 2018. /https://econpapers.repec.org/paper/zbwwtowps/ersd 201803.htm
64. Kallender and Hughes, 2017. /https://www.tandfonline.com/doi/abs/ 10.1080/01402390.2016.1233493
65. Brenner and Koops, 2004. /https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=786507
66. Frischmann, 2003. /https://lawecommons.luc.edu/luclj/vol35/iss1/8/
67. Kerr, 2003, /https://www.unodc.org/e4j/data/university_uni/the_ problem_of_perspective_in_internet_law.html?lng=en
68. Report of the Working Group on Internet Governance. Château de Bossey. June 2005. (WGIG, 2005). /https://www.wgig.org/docs/WGIGREPORT.pdf
69. Enisa 2014. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
70. Enisa 2017./ https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
71. NIST 2012./ https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1
72. NIST 2018. /https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
73. Leukfeldt et al., 2017. /https://www.researchgate.net/publication/ 320323730_The_Use_of_Online_Crime_Markets_by_Cybercriminal_Networks_A_View_From_Within
74. Leukfeldt, Lavorgna, and Kleemans, 2017. /https://www.researchgate.net/publication/309960777_Organised_Cybercrime_or_Cybercrime_that_is_Organised_An_Assessment_of_the_Conceptualisation_of_Financial_Cybercrime_as_Organised_Crime

75. Arsovska, 2011./ https://journals.sagepub.com/doi/abs/10.1177/ 00943061103917641
76. Whiteman, 2012. /https://www.tandfonline.com/doi/abs/10.1080/14780887.2015.1008913

Подписано в печать 04.07.2022. Формат 60x84 1/16.
Бумага офсетная. Усл. печ. л. 9,75. Тираж 500 экз. Заказ № 3879.
Отпечатано в ТОО «Издательство LEM»
050008, г. Алматы, ул. Ауэзова, 82, уг. ул. Мынбаева, тел./факс 375-51-33.