Список использованных источников:

1. Самые громкие кибер-атаки на критические инфраструктуры. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/panda/blog/316500/

2. Каждая вторая компания в России теряет важные данные из-за кибератак. [Электронный ресурс]. – Режим доступа: http://www.kaspersky.ru/about/ news/virus/2016/losing-important-data-because-of-cyber-attacks

3. Тренды DDOS-атак 2015-2016. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/webo/blog/309476/

4. Сычев А. Киберустойчивость. Что это такое? Презентации участников IX Уральского форума «Информационная безопасность финансовой сферы» [Электронный ресурс]. – Режим доступа: https://ural.ib-bank.ru/materials2017

5. Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity [Электронный ресурс]. – Режим доступа: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

6. Cisco 2017 Annual Cybersecurity Report. [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/dam/m/digital/en_us/Cisco_Annual_Cybersecurity_Report_2017.pdf

7. Integration of Digital Technology in the EU 2016. [Электронный ресурс]. – Режим доступа: https://ec.europa.eu/digital-single-market/en/integration-digital-technology

8. Staying ahead on cyber security [Электронный ресурс]. – Режим доступа: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/staying-ahead-on-cyber-security

9. В 2016 году количество киберугроз в мире достигло рекордной отметки за всю историю - Trend Micro. [Электронный ресурс]. – Режим доступа: http://www.finmarket.ru/news/4478855

10. Computer Emergency Response Team Coordination Center, Carnegie Mellon University, Pittsburgh, 2002.

11. Risk and Responsibility in a Hyperconnected World. [Электронный ресурс]. – Режим доступа:http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

УДК 004.632

Е.Д. Семенова,
канд. экон. наук, доцент кафедры статистики,
К.И. Тарасова,
канд. экон. наук, преп. кафедры статистики,
старший научный сотрудник научно-исследовательской части,
Одесский национальный экономический университет, Украина, г. Одесса.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

INFORMATION SECURITY AS A COMPONENT OF THE ECONOMIC SECURITY OF THE STATE

Рассмотрены этапы развития информационной безопасности в мире, начиная с периода Второй мировой войны и закачивая условиями современности. Проанализировано текущее состояние Интернет-угроз, охарактеризованы наиболее уязвимые пользователи глобальной сети.

***Ключевые слова*:** информационная безопасность, безопасность данных, кибер-атака, глобальная сеть, Интернет.

The stages of the development of information security in the world beginning with the period of the Second World War and uploading the conditions of the present are viewed. The current state of Internet threats is analyzed, the most vulnerable users of the global network are characterized.
***Keywords*:** Information security, data security, cyber-attack, global network, the Internet.

История информационной безопасности начинается с компьютерной безопасности, потребность в которой, возникла во время Второй мировой войны, когда были использованы первые мейнфреймы, разработанные для вычисления кодов. В то время для защиты и сохранения целостности информации были использованы несколько уровней систем защиты, а доступ, например, к конфиденциальным военным локациям контролировался при помощи значков, ключей и распознавания лиц уполномоченного персонала.

Растущая необходимость поддержания национальной безопасности в конечном итоге привела к более технологически сложным гарантиям информационной безопасности. В начальном периоде безопасность данных представляла собой простой процесс, состоящий преимущественно из физической безопасности и простых схем классификации документов. Основными же угрозами являлись шпионаж, физическое хищение оборудования и саботаж.

Во время холодной войны множество других мейнфреймов было подключено к сети для выполнения все более сложных задач, что привело к необходимости взаимодействия при помощи менее громоздкого процесса, чем рассылка магнитных лент между компьютерными центрами. В ответ на эту необходимость Управление перспективных исследовательских проектов министерства обороны США (DARPA) приступило к изучению возможности создания сетевой коммуникационной системы для поддержки военного обмена информацией, а Ларри Робертс разработал проект под названием ARPANET, который послужил предшественником Интернета [1, с. 4].

На протяжении следующих двух десятилетий ARPANET становился все более популярным, однако рос и потенциал для его негативного использования. В 1973 г. Робертом Меткалфом были выявлены фундаментальные проблемы безопасности данной системы: отдельные удаленные сайты не располагали достаточными средствами контроля для защиты данных от несанкционированных удаленных пользователей; структура и формат паролей были уязвимыми; для коммутируемых соединений отсутствовали процедуры безопасности; а идентификация пользователей и авторизация в системе была невозможной. Таким образом, из-за огромного диапазона возможных атак и частоты нарушения компьютерной безопасности, сеть была признана как носящая угрозу, что повлекло за собой всевозможные исследования и публикации в сфере безопасности данных. К наиболее важным из них следует отнести «Предварительные замечания по разработке безопасных военных компьютерных систем» Роджера Шелла, Питера Дауни и Джеральда Попека, «Защита паролем: история дела» Роберта Морриса и Кена Томпсона, «Защита данных файла» Дениса Ритчи и так далее.

В ноябре 1988 г. и так небезопасная ARPANET была парализована сетевым червем, который задел более шести тысяч узлов сети, что позволило усиленными темпами развиваться её главному конкуренту – NSFNet, обширной межуниверситетской сети, которая имела гораздо большую пропускную способность. Уже к 1990-му г. ARPANET прекратила свое существование, и в этот же период было зафиксировано первое подключение к всемирной паутине Интернет, концепция которой была разработана годом ранее в стенах Европейского совета по ядерным исследованиям британским ученым Тимом Бернесом-Ли. Так, девяностые годы двадцатого столетия ознаменовали новую веху в истории информационной безопасности.

В конце двадцатого века сети компьютеров становятся все более распространенными, а необходимость подключения этих сетей друг к другу растет. Это и приводит к появлению Интернета, первой глобальной сети сетей. Уже к концу 1990-х годов Интернет становится доступным широкой общественности, хотя ранее он являлся сферой деятельности правительства, академических кругов и специализированных отраслевых специалистов.

С момента своего создания в качестве инструмента для обмена информацией Интернет трансформируется в соединение миллионов сетей. Первое время эти соединения были основаны на стандартах де-факто, потому что в то время отраслевых стандартов для объединения сетей не существовало. Эти де-факто стандарты мало обеспечивали безопасность информации; во времена развития Интернет безопасность данных вообще имела низкий приоритет. На самом деле, многие из проблем, с которыми сегодня сталкивается, к примеру, электронный обмен писем, являются результатом такого раннего отсутствия безопасности. В то время, когда все пользователи сети и электронной почты были преимущественно ученые, аутентификация почтового сервера и шифрование электронной почты не представлялись необходимыми. Ранние вычислительные подходы полагались на безопасность, которая была встроена в физическую среду центра обработки данных, в которой и размещались компьютеры. Сейчас, поскольку сетевые компьютеры стали доминирующим стилем вычислений, способность физически обезопасить сетевой компьютер была утрачена, а хранимая информация стала более уязвимой для угроз безопасности.

Сегодня Интернет приводит миллиарды небезопасных компьютерных сетей в непрерывную связь друг с другом: согласно данным Мирового банка в 2016 г. численность пользователей сети составила 3,5 млрд. человек [2]. Безопасность хранимой информации каждого персонального компьютера теперь зависит от уровня безопасности любого другого компьютера, к которому он подключен.

В последние годы растет осознание необходимости повышения информационной безопасности, а также осознание того, что защита информации важна для экономической и политической безопасности любого государства. Растущая угроза кибер-атак заставила правительства и компании острее осознавать

необходимость защиты контролируемых компьютером систем управления коммунальными предприятиями и другой критически важной инфраструктурой страны.

Среди исследователей и практиков в сфере информационной безопасности крепнет признание того, что пользователям сети практически невозможно блокировать все атаки, направленные на них. Учитывая крайне постоянный и целенаправленный характер большинства современных кибер-атак, многие ученые считают, что нарушение безопасности данных практически неизбежно для большинства организаций. Независимо от того, насколько хорошо защищена организация, опытный противник всегда найдет способ проскользнуть внутрь ее системы просто потому, что современные сети настолько велики, сложны и взаимосвязаны, что почти невозможно сохранить каждую точку входа постоянно безопасной.

Одной из самых больших проблем, с которой сталкиваются предприятия сегодня, является анализ всех данных, генерируемых различными системами безопасности в Интернет-сетях. Антивирусные средства, системы обнаружения и предотвращения вторжений, унифицированные устройства для управления угрозами и другие технологии могут генерировать множество дополнительных данных, с которыми проблематично справиться даже администраторам по информационной защите. Если добавить к этому разговоры с мобильных устройств, информацию виртуализированных систем и облачных ресурсов, объем данных может стать для организации подавляющим.

Более того, по данным компании Hewlett Packard, в среднем предприятия получают еженедельно 17 тыс. предупреждений о вредоносном программном обеспечении, подавляющее большинство которых оказывается ложным [3]. Для крупных компаний преследование таких ложных предупреждений обходится порядка 1,3 млн. дол. США в год. Фактически, только 19 % процентов предупреждений, генерируемых системами безопасности, обычно надежны, а из-за огромного объема данных администраторы в конечном итоге смотрят лишь около 4 % уведомлений, которые они получают, создавая огромную уязвимость для организаций.

Так в 2016 г. было зарегистрировано 4149 нарушений в различных крупных системах, которые обнародовали более 4,2 млрд. личных данных пользователей. В то же время ущерб мировой экономике от хищений того или иного типа информации составил порядка 445 млрд. долл. Наибольший ущерб был нанесен таким компаниям, как Yahoo, MySpace, Adobe Systems, eBay, LinkedIn и так далее. Именно на бизнес-сектор приходится наибольшее количество кибер-атак (51 %), второе место занимает правительственный сектор (23 %), третье – медицинский сектор (12 %) [4, с. 1]. Однако из этого вовсе не следует, что в большинстве своем риску опасности данных подвержены крупные компании и корпорации. С наибольшим риском потери данных сталкиваются именно мел-

кие и средние фирмы, при помощи которых опытные хакеры, впоследствии, ищут доступ к более закрытым системам.

В заключение следует отметить, что с течением времени проблема информационной безопасности приобретает все большую актуальность, а в современных реалиях компьютерные преступления являются составной частью всех угроз негативного информационного влияния. В отличие от любой другой программы в области информационных технологий, основной задачей информационной безопасности является обеспечение того, чтобы системы и их содержимое оставались неизменными. Предприятия используют сотни тысяч долларов и тысячи человеко-часов для поддержания своих информационных систем. Атаки на информационные системы являются повседневным явлением, а потребность в информационной безопасности растет вместе с изощренностью таких атак. Предприятия должны понимать среду, в которой работают информационные системы, чтобы их программы информационной безопасности могли предотвращать потенциальные угрозы, что обуславливает актуальность изучения вопроса безопасности данных и проблем ее обеспечения.

Список использованных источников:

1. Introduction to information security [Electronic resource]. – Available at:http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf (date of appeal: 09.03.17). – Title screen.

2. Global Economic Prospects. June 2016. Divergences and Risks [Electronic resource]. – 2016. – № 26. – Available at: http://pubdocs.worldbank.org/en/842861463605615468/Global-Economic-Prospects-June-2016-Divergences-and-risks.pdf (date of appeal: 09.03.17). – Title screen.

3. Hewlett Packard website – Available at: http://www.hp.com/country/us/en/welcome.html – Title screen.

4. Data Breach QuickView Report. 2016 Data Breach Trends – Year In Review. [Electronic resource]. – 2017. – Available at: https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf (date of appeal: 09.03.17). – Title screen.

УДК 004.9

С.Г. Федорченко,
канд. техн. наук, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем,
Инженерно-технический институт, ПГУ им. Т.Г. Шевченко.

РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРИДНЕСТРОВЬЕ

DEVELOPMENT OF INFORMATION TECHNOLOGIES IN TRANSNISTRIA

Рассматривается положение в ИТ-индустрии ПМР. Предлагается использовать опыт Белоруссии.
***Ключевые слова*:** ИТ-индустрия, подготовка кадров.