- формирования отчетности по рискам;
- определения размера резерва на возможные потери / потери по ссудам;
- ценообразования с учетом оценки потерь по кредитному риску;
- оценки уровня ожидаемых и непредвиденных потерь;
- расчета экономического капитала.

Библиографические ссылки

1. Банковский кодекс Республики Беларусь: с изм. и доп. по состоянию на 19 ноября 2018 г. Минск : Нац. центр правовой информ. Респ. Беларусь, 2019. 224 с.
2. Lyn Thomas C. Consumer credit Models: Pricing, Profit, and Portfolios // Oxford University Press. 2009.
3. Thomas C. Wilson. Portfolio credit risk // FRBNY Economic Policy Review. October, 1998.
4. Гичан О. С., Господарик Е. Г. Современная практика разработки скоринговых карт для розничных клиентов в белорусских банках // Банк. весн. 2020. № 4/681. С. 49–59.

УДК 004.056

ЭКОНОМИЧЕСКИЙ АСПЕКТ КИБЕРПРЕСТУПНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ

М. Г. Головенчик

Магистр права, преподаватель Юридического колледжа Белорусского государственного университета», г. Минск

Научный руководитель: **Т. Н. Михалёва**

Кандидат юридических наук, доцент, доцент кафедры государственного управления, декан юридического факультета Белорусского государственного университета, г. Минск

Развитие цифровых технологий породило одну из самых опасных угроз, с которыми в последние годы сталкивается международное сообщество, – преступность в киберпространстве. В статье кратко проанализированы виды и экономические последствия кибератак, отмечена важность международного сотрудничества в борьбе с компьютерными преступлениями, определены перспективные направления борьбы с киберпреступностью.

Ключевые слова: цифровые технологии; цифровизация; киберпреступность; кибератака; киберугроза.

ECONOMIC ASPECT OF CYBERCRIME: CURRENT STATE AND MODERN TRENDS

M. G. Goloventchik

Master of Law, Lecturer of Law College of the Belarusian State University, Minsk

Supervisor: **T. N. Mikhaleva**

PhD in Law, Associate Professor of Public Administration Department, Dean of the Faculty of Law of the Belarusian State University, Minsk

The development of digital technologies has created one of the most dangerous threats that the international community has faced in recent years – crime in cyberspace. The article briefly analyzes types and economic consequences of cyberattacks, highlights the importance of international cooperation in the fight against computer crimes, and identifies areas for combating cybercrime.

Keywords: Digital technology; digitalization; cyber crime; cyber attack; cyber threat.

За последние несколько десятилетий человечество сделало значительный прорыв в развитии науки и технологий, в особенности в тех отраслях, которые связаны со способами хранения и передачи информации, автоматизации технологических процессов, цифровизации государственной, политической, экономической, общественной и иных сфер жизнедеятельности.

Глобальная цифровизация благоприятно отражается на мировой экономике, производя существенные положительные изменения, связанные со значительным расширением рынков сбыта продукции, работ, услуг.

Вместе с тем, виртуальное пространство, благодаря которому мы сегодня имеем возможность реализовывать многочисленные возможности, является также инструментом, позволяющим дистанционно (а фактически – трансгранично) получать доступ к любым данным, хранящимся в виде машинного кода. В результате складывается ситуация, когда рост возможностей, предоставляемых глобальной цифровизацией, пропорционально увеличивает потенциал кибератак, которым могут быть подвержены различные объекты, наиболее значимые в сфере государственной или общественной жизни. Так, «…кибератаки могут дестабилизировать общественно-политическую обстановку, инспирировать и поддерживать протестную активность граждан…» [1]. Стремительное развитие рынков товаров, работ и услуг, сопровождающееся возможностью осуществления мгновенных безналичных платежей, повлекло за собой появление нового вида преступности – киберпреступности.

Следует отметить, что киберпреступность относится к угрозам, с которыми сопряжена глобальная цифровизация бизнес-процессов. Анализируя возможные риски в экономической сфере, связанные с переходом на цифровые информационные технологии, к числу современных экономических киберугроз можно отнести «атаки на банки, атаки на брокера, атаки на расчетную систему, хищения через интернет-банкинг, неправомерное использование бренда, применение программы-вымогателя и некоторые другие действия, совершаемые посредством использования вредоносных программ» [3].

В 16-м издании Отчета о глобальных рисках, опубликованного в 2021 г. Всемирным экономическим форумом [6], приведены данные о количестве глобальных «значительных» кибератак, произошедших с мая 2006 г. по июнь 2020 г. «Значительные» кибератаки представляют собой кибератаки на правительственные учреждения страны, оборонные и высокотехнологичные компании или экономические преступления с потерями в размере более одного миллиона долларов (рис. 1).

Так, аналитики Specops Software, проанализировав последние данные Центра стратегических и международных исследований (CSIS) [5], отмечают, что за вышеуказанный период в США произошло 156 наиболее значительных кибератак. В то же время в Великобритании произошло 47 кибератак, классифицированных как «серьезные», включая крупномасштабные кибератаки, развернутые на цифровых платформах Лейбористской партии во время всеобщих выборов 2019 г. Индия в данном рейтинге занимает третье место, в стране за названный период произошло 23 «значительные» кибератаки.

Согласно совместной оценке CSIS и McAfee [7], с 2018 г. стоимость глобальной киберпреступности превысила 1 трлн долл. США, а понесенные убытки от достигли примерно 945 млрд долл. США (рис. 2).

Более того, как отмечают аналитики Cybersecurity Ventures, ежегодный глобальный ущерб от киберпреступности к 2025 г. достигнет 10,5 трлн долл. США [4].

Необходимо отметить, что глобализация мировой экономики является безусловно важным (если не ключевым) фактором ее дальнейшего развития. Фактическая денонсация государственных границ при формировании новых (глобальных) рынков сбыта на сегодняшний день уже воспринимается как естественное явление. Однако нормальное

функционирование экономики в новых условиях станет возможным только тогда, когда большинство (в идеале – все) государств объединят свои усилия в деятельности по противодействию компьютерной преступности [2]. Сегодня же многие компании (и это касается всех без исключения мировых держав, как развитых, так и находящихся в стадии развития) все еще остаются уязвимыми для вновь возникающих киберугроз, что обусловлено использованием устаревших механизмов и технологий, недостаточной технической подготовленностью персонала, а также банальной халатностью, допускаемой работниками компании, так или иначе осуществляющими свою деятельность во всемирной глобальной сети, и отсутствием «цифровой культуры».

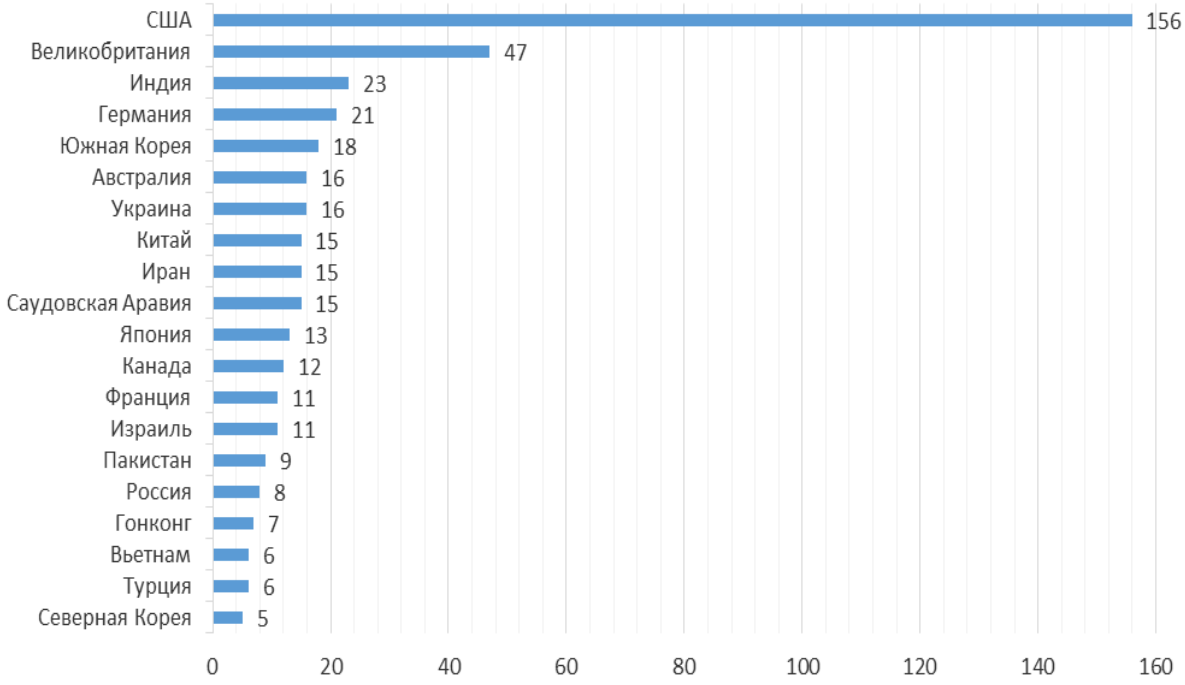

Рисунок 1 – **Данные о количестве глобальных «значительных» кибератаках, произошедших с мая 2006 г. по июнь 2020 г.**

Примечание – Разработка автора на основе [6].

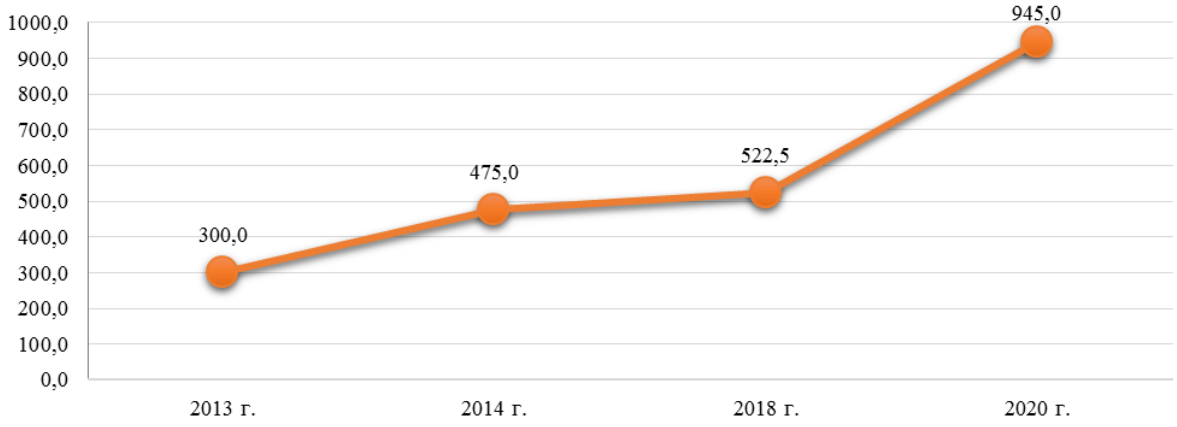

Рисунок 2 – **Расчетная средняя стоимость киберпреступности, млрд долл. США**

Примечание – Разработка автора на основе [7].

Характеризуя межгосударственные усилия, направленные на борьбу с проявлениями трансграничной киберпреступности, следует отметить, что на сегодняшний день большинство мировых держав понимают опасность этого явления и предпринимают определенные шаги к тому, чтобы противостоять ей. Вместе с тем, нельзя не отметить, что, во-первых, вплоть до настоящего времени не было разработано единого международного документа, посвященного данной проблеме – все существующие международные соглашения в этой области носят лишь региональный характер. Во-вторых, даже имеющиеся дву- и многосторонние соглашения, распространяющие свое действие на определенный регион, как правило, существенно отстают в своем правовом регулировании от стремительно развивающегося технического прогресса.

Таким образом, для успешной борьбы с международной киберпреступностью, которую, без сомнения, можно отнести к числу глобальных проблем современности, требуется, во-первых, унификация подходов к пониманию самой сущности этого явления, во-вторых, активизация усилий всех без исключения государств, направленных на оперативную модернизацию внутреннего законодательства и разработку глобального международного соглашения, нормы которого регулировали бы складывающиеся отношения в рассматриваемой сфере, в-третьих, государственное финансирование программ, направленных на выявление киберпреступлений и изобличение киберпреступников, в-четвертых, повышение уровня осведомленности в области кибербезопасности как государственных органов и компаний, так и граждан.

Библиографические ссылки

1. Головенчик М. Г., Краско Г. Г., Головенчик Г. Г. Проблемы кибербезопасности умных городов // Наука и инновации. 2020. № 12 (214). С. 54.

2. Головенчик М. Г., Головенчик Г. Г., Старовойтов О. М. Угрозы киберпреступности в современных условиях глобализации мировой экономики // Сб. тезисов 77-й науч.-практ. конференции студентов, магистрантов и аспирантов факультета международных отношений БГУ. Минск, 23 апреля 2020 г. / Редкол.: В. Г. Шадурский [и др.]. Минск, 2020. С. 700.

3. Грачева Ю. В. Цифровизация: некоторые уголовно-правовые риски в сфере экономики // Уголовное право. 2019. № 5. С. 28.

4. Cybercrime to cost the world $10.5 trillion annually by 2025 // Cybersecurity Ventures : [site]. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (date of access: 25.01.2021).

5. The countries experiencing the most ‘significant’ cyber-attacks // Specops Software : [site]. URL: https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/ (date of access: 25.01.2021).

6. The Global Risks Report 2021 // WEF : [site]. URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (date of access: 25.01.2021).

7. The Hidden Costs of Cybercrime // McAfee : [site]. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf (date of access: 25.01.2021).

УДК 33.338

АНАЛИЗ ГОСУДАРСТВЕННЫХ УСЛУГ В СИСТЕМЕ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ

Е. Э. Головчанская[1)], П. В. Дударева[2)]

[1)] *Кандидат экономических наук, доцент,*
доцент кафедры аналитической экономики и эконометрики
экономического факультета Белорусского государственного университета, г. Минск

[2)] *Студентка экономического факультета*
Белорусского государственного университета, г. Минск