

ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

А. М. Халимончик

*студент специальности «Финансы и кредит», экономический факультет,
Белорусский государственный университет, г. Минск, Республика Беларусь,
e-mail: arinakhal24@gmail.com*

Научный руководитель: С. Н. Костюкова

*кандидат экономических наук, доцент, Белорусский государственный университет,
г. Минск, Республика Беларусь, e-mail: Kostjukova@bsu.by*

В связи с постоянным совершенствованием и внедрением информационно-компьютерных технологий, возрастает опасность становления жертвой преступников в виртуальном пространстве. Преступления, совершаемые в сфере информационно-компьютерных технологий, называются киберпреступностью. В статье рассмотрена актуальность киберпреступности, а также проанализирована динамика изменения числа киберпреступлений на современном этапе в Республике Беларусь.

Ключевые слова: киберпреступность; кибербезопасность; кибератаки; киберинциденты; цифровизация; информационно-компьютерные технологии.

CYBERSECURITY ISSUES IN MODERN CONDITIONS

A. M. Khalimonchik

*Student of the Department of «Corporate Finance», Economic Faculty,
Belarusian State University, Minsk, Republic of Belarus, e-mail: arinakhal24@gmail.com*

Supervisor: S. N. Kostiukova

*PhD in Economic, Associate Professor, Belarusian State University, Minsk,
Republic of Belarus, e-mail: Kostjukova@bsu.by*

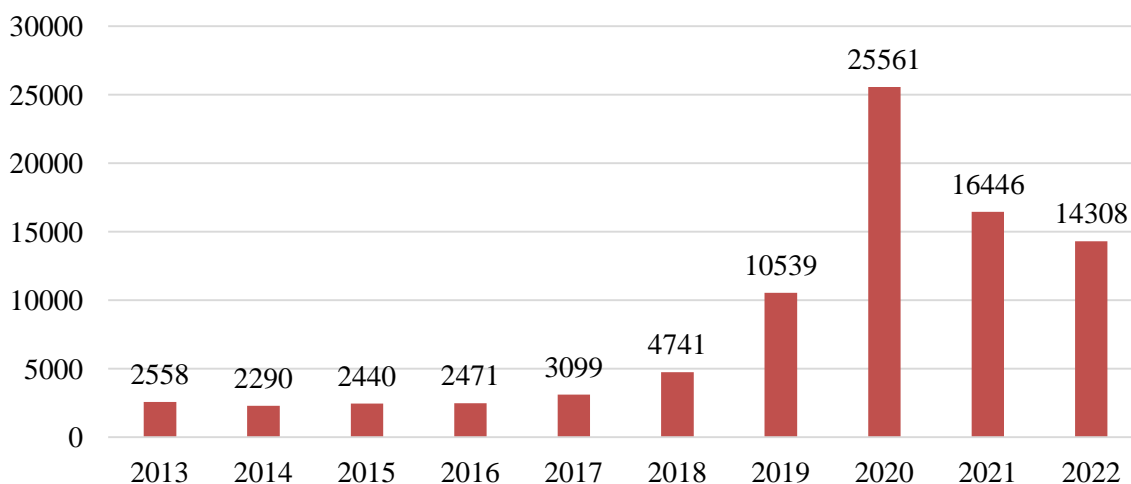
Due to the constant improvement and introduction of information and computer technologies, the danger of becoming a victim of criminals in the virtual space increases. Crimes committed in the field of information and computer technology are called cybercrime. The article considers the relevance of cybercrime, as well as analyzes the dynamics of changes in the number of cybercrimes at the present stage in the Republic of Belarus.

Keywords: cybercrime; cybersecurity; cyberattacks; cyber incidents; digitalization; information and computer technologies.

Мы живем в эру цифровизации, где с каждой секундой растет значение Интернета и компьютерных технологий. Вместе с этим растут как перспективы граждан и общества в целом, так и возникают новые риски и угрозы. Стремительное развитие цифровых технологий, рост используемой электронной техники, устройств и услуг привело к значительному росту количества киберпреступлений.

Киберпреступность – одна из наиболее быстрорастущих сфер экономической преступности. Это связано с ростом количества пользователей сети Интернет, внедрение в разные отрасли производства программируемых машин и устройств, повышением профессионализма киберпреступников [4].

Киберпреступность является серьезной проблемой и для Беларуси. Первое преступление к данной сфере было совершено в 2002 году. С того времени наблюдался устойчивый рост киберпреступлений, который пошел на спад только в 2021 году.



Статистические сведения о киберпреступности в Республике Беларусь за 2013–2022 гг.

Собственная разработка автора на основе данных МВД Республики Беларусь [3].

Анализируя диаграмму, можно сделать вывод о том, что наибольшее число киберпреступлений наблюдалось в 2020 году. Рост числа преступлений в этом году по сравнению с 2019 составил 15 022, что говорит об увеличении на 142,54 %. По результатам 2021 года произошел значительный спад на 35,66 % (9115). В 2022 количество зарегистрированных киберпреступлений продолжило снижаться, сокращение составило 13 % или 2 138 преступлений.

По оценкам экспертов в течение последних нескольких лет, ввиду стремительного развития информационных технологий в 2023 году сохранится тенденция совершения значительного числа киберпреступлений.

Присутствие киберпреступности в Беларуси обусловлено рядом причин: интенсивно идёт процесс развития системы безналичных расчётов, появляется все больше устройств, осуществляющих финансовые транзакции, увеличивается количество пользователей электронных платежных систем, держателей банковских платежных карт, интернет-пользователей, абонентов сотовой связи [7].

Также одной из основных причин роста преступлений в киберсфере является недостаточная цифровая грамотность граждан в сфере защиты персональных данных при отсутствии базовых знаний по общим методам распространения вредоносных компьютерных программ и программных продуктов, что приводит к тысячам случаев, когда граждане Республики Беларусь становятся жертвами, а принадлежащие им технические средства – орудиями противоправного использования информационно-компьютерных технологий [6].

В 2020 году британская компания Comparitech изучила 76 стран и выяснила, в какой стране наименее низкий уровень кибербезопасности. Для ранжирования стран применялось несколько параметров: какой процент мобильных устройств и ПК в стране инфицирован вредоносными ПО, число кибератак на финансовые институты, качество ИБ-законодательства в стране, также ряд других параметров. В десятке стран с худшими показателями кибербезопасности Беларусь заняла 6-е место. Экспертами отмечена крайне высокая вероятность заражения вредоносным ПО смартфонов и компьютеров белорусских пользователей – 9,33 % и 31,1 %, соответственно. Также было отмечено, что максимальное количество кибератак на финансовый сектор по странам пережила Беларусь (2,9 %). Уже в 2022 году Беларусь улучшила свое положение на 29 позиций и заняла 35-е место [8].

14 февраля 2023 года Президентом Республики Беларуси был подписан Указ № 40 «О кибербезопасности» [5].

В целях повышения уровня защиты национальной информационной инфраструктуры было принято решение о создании национальной системы обеспечения кибербезопасности. Таким образом в Беларуси появится Национальный центр кибербезопасности, который будет создан в структуре Оперативно-аналитического центра при Президенте РБ.

Кроме того, Указ № 40 содержит перечень владельцев критически важных объектов информатизации. Вошедшие в него юридические лица, а также поставщики услуг хостинга официальных интернет-сайтов и электронной почты должны будут в течение года после вступления Указа в силу создать свои внутренние центры кибербезопасности. В Перечень вошло 27 организаций, в их числе: три банка (Беларусбанк, Белагропромбанк, Белгазпромбанк), Банковский процессинговый центр, БМРЦ,

Белгосстрах, ООО «Белорусские облачные технологии», БелАЭС и все РУП электроэнергетики областного уровня, Белтелеком, операторы связи А1 и МТС, несколько предприятий реального сектора экономики (например, ОАО «Гродно Азот», «Нафтан») [5].

Таким образом, развитие киберпреступности идет в ногу с развитием информационно-технических средств. Множество отраслей завязаны на кибербезопасности, и в этой связи важно обеспечить защиту промышленной отрасли, реального сектора экономики, государственных органов и организаций. Решению этой задачи служит Указ № 40 «О кибербезопасности». Реализация мер, предусмотренных в Указе, позволит консолидировать усилия по предотвращению, обнаружению и минимизации последствий кибератак на объекты информационной инфраструктуры, тем самым повысить безопасность и надежность информационных систем страны.

Библиографические ссылки

1. Юридический словарь [Электронный ресурс]. URL: <http://multilang.etalonline.by/ru> (дата обращения 10.04.2023).

2. Постановление совета безопасности Республики Беларусь 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» [Электронный ресурс]. URL: <https://pravo.by/document/?guid=12551&p0=P219s0001&p1=1>

3. Министерство внутренних дел Республики Беларусь [Электронный ресурс]. URL: <https://www.mvd.gov.by/ru> (дата обращения 10.04.2023).

4. *Кобец П. Н.* Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения // Вестник Самарского юридического института. 2022. № 1 (47). [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/kiberprestupnost-sovremennye-vidy-prichiny-ee-porozhdayuschie-i-osobennosti-preduprezhdeniya/viewer> (дата обращения 10.04.2023).

5. Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» [Электронный ресурс]. URL: <https://president.gov.by/bucket/assets/uploads/documents/2023/40uk.pdf> (дата обращения 10.04.2023).

6. *Шпанькова Д. А.* Проблемы обеспечения кибербезопасности в Республике Беларусь: экономические и социальные аспекты; науч. рук. В. В. Клейман // Беларусь в современном мире: материалы XV Междунар. науч. конф. студентов, магистрантов, аспирантов и молодых ученых, Гомель, 19–20 мая 2022 г. / М-во образования Респ. Беларусь, Гомел. гос. техн. ун-т им. П. О. Сухого, Гомел. обл. орг. «Белорус. о-во «Знание»; под общ. ред. В. В. Кириенко. Гомель: ГГТУ им. П. О. Сухого, 2022.

7. *Головенчик Г. Г.* Проблемы обеспечения кибербезопасности в Республике Беларусь / Беларусь в современном мире = Беларусь у сучасным свеце: материалы XVII Междунар. науч. конф., посвящ. 97-летию образования Белорус. гос. ун-та, Минск, 26 окт. 2018 г. / Белорус. гос. ун-т; редкол.: В. Г. Шадурский (пред.) [и др.]. Минск: БГУ, 2018. С. 162–163.

8. Which countries have the worst (and best) cybersecurity? [Электронный ресурс]. URL: <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/> (дата обращения 12.04.2023).