УДК 338

***В.Ю. Циклаури, Л.С. Белоусова, И.Н. Родионова***

Юго-Западный государственный университет, Курск, email: vika-ts@mail.ru

# КИБЕРПРЕСТУПНОСТЬ КАК СЛЕДСТВИЕ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

**Ключевые слова:** безопасность в киберпространстве, информационная безопасность, киберпреступления в сети.

Вследствие стремительного технологического прогресса закономерно возникают важные вопросы по организации процессов обработки, хранения, распространения и защиты информации в глобальных информационно-коммуникационных системах. На данный момент общество сталкивается с фактом возрастающих угроз кибербезопасности, что делает вопрос кибербезопасности важным, как в национальном, так и в международном контексте. Цель исследования заключается в изучении современного состояния и оценки угроз информационной безопасности в условиях развития цифровой экономики, влияния киберпреступности на безопасность государства, а также в разработке рекомендаций по учету Россией будущего направления соответствующих трендов. Авторами систематизированы показатели характеризующие количество официально зарегистрированных преступлений в 2017–2022 гг., совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации; преступлений, совершенных с использованием или применением (пластиковых) карт; преступлений, совершенных с использованием или применением компьютерной техники; преступлений, совершенных с использованием или применением программных средств; преступлений, совершенных с использованием или применением фиктивных электронных платежей; преступлений, совершенных с использованием или применением сети «Интернет»; преступлений, совершенных с использованием или применением средств мобильной связи. В исследовании применен комплекс общенаучных подходов (абстрактно-логический, дедуктивный, комплексный и системный). Реализация процесса исследования осуществлялась при помощи диалектического метода познания, предопределяющего изучение экономических явлений в их взаимосвязи и развитии. Для решения отдельных задач применялись экономико-статистические методы, методы сравнения, абсолютных, относительных величин, табличного представления данных.

***V.Y. Tsiklauri, L.S. Belousova, I.N. Rodionova***

South-Western State University, Kursk, email: vika-ts@mail.ru

# CYBER CRIME AS A CONSEQUENCE OF DIGITALIZATION OF THE ECONOMY

**Keywords:** security in cyberspace, information security, cybercrime on the network.

Due to rapid technological progress, important questions naturally arise regarding the organization of processes for processing, storing, distributing and protecting information in global information and communication systems. In this context, it is worth noting that at the moment society is faced with the fact of increasing threats to cybersecurity, which manifests itself with a threat to the security of information, knowledge on the Internet, protection from cyber threats, countering espionage, sabotage, countering the growth of crime and fraud on the Internet, which makes the issue cybersecurity is an important issue in both national and international contexts. The purpose of the study is to study the current state and assess the threats to information security in the context of the development of the digital economy, the impact of cybercrime on state security, as well as to develop recommendations for Russia to take into account the future direction of relevant trends. The authors systematized indicators characterizing the number of officially registered crimes in 2017–2022, committed using information and telecommunication technologies or in the field of computer information; crimes committed with the use or application of (plastic) cards; crimes committed with the use or application of computer technology; crimes committed with the use or application of software; crimes committed with the use or application of fictitious electronic payments; crimes committed using or using the Internet; crimes committed with the use or application of mobile communications. The study used a complex of general scientific approaches (abstract-logical, deductive, complex and systemic). The implementation of the research process was carried out using the dialectical method of cognition, which predetermines the study of economic phenomena in their interrelation and development. To solve individual problems, economic and statistical methods, methods of comparison, absolute, relative values, and tabular presentation of data were used.

Развитие информационных технологий породило как положительные тенденции, связанные с их успешным использованием в различных сферах жизнедеятельности общества, так и негативные, сопряженные с их применением как в качестве объекта (предмета) преступления, так и орудия, средства совершения преступления. Использование информационных технологий в преступных целях сопряжено с созданием для государства современных угроз, требующих соразмерного и эффективного ответа.

С развитием ИКТ, ИТС и глобальной сети Интернет мировое сообщество, получив невиданные до этого возможности в плане обмена информацией, стало чрезвычайно уязвимым из-за стороннего кибернетического воздействия, а именно в отношении фактически нескрываемых попыток влияния противоборствующих сторон на информационное и киберпространства друг друга за счет использования средств современной вычислительной или специальной техники и соответствующего программного обеспечения – кибервмешательств, а также других проявлений их дестабилизирующего воздействия на тот или иной объект, совершаемого за счет технологических возможностей информационного и киберпространства, с созданием опасности, так называемых киберугроз, как для этого пространства, так и для сознания каждого человека [1].

Особенности распространения информации, возможности неограниченного и неконтролируемого ее влияния, несанкционированный доступ, компьютерные вирусы остро поставили перед обществом проблемы информационной безопасности. Информационная безопасность должна осуществляться комплексно и систематически с использованием полного набора организационных, технических, аппаратно-программных и иных средств. Становление общества нового информационного формата остро ставит вопрос информационной безопасности пространства государства, человека, общества [2]. Информационная безопасность приобретает особое значение и вследствие тесного взаимодействия с экономической и национальной безопасностью вносит значительный вклад в глобальную безопасность.

Массовое распространение компьютеров и появление информационных сетей спровоцировало появление нового вида преступности – киберпреступность. Размер вреда от экономических киберпреступлений очень высок, что свидетельствует о повышенной степени общественной опасности таких преступлений. Однако данным цифрам может быть и иное объяснение: один человек с возможностями киберпространства может совершить гораздо больше преступлений, нежели без таких возможностей. Так, например, за одно и то же время хакер может совершить десять хищений, в то время как обычный преступник – всего одно. Также с возможностями киберпространства виновный может одновременно совершать преступления по отношению сразу к нескольким протерпевшим, приумножая тем самым причиняемый вред [4].

## Объекты и методы исследования

Объект исследования – процесс оценки влияния киберпреступности на безопасность государства.

Представленная работа выполнена с применением общепринятых теоретических методов научного познания. Проведенное исследование в основном базируется на использовании экосистемного подхода, а также сравнительного анализа открытых источников, что соответствует поставленным в работе цели и задачам, и, в конечном итоге, позволило определить основные цели, задачи, планы, проекты, масштабы и методологию оценки конкурентоспособности, на уровне рассматриваемых в статье государств.

## Результаты и их обсуждение

Говоря о масштабах киберпреступности необходимо отметить следующее. Так согласно официальным статистическим данным ФКУ «ГИАЦ МВД России» в 2018 г. каждое 11-12 (8,8 % 174 674 из 1 991 532) зарегистрированное преступление относилось к числу киберпреступлений, в 2019 это было каждое седьмое (14,5 % 294 409 из 21 024 337), а в 2020 г. – каждое четвертое (25,0 % 510 396 из 2 044 221). Таким образом, в 2022 году число преступлений в сфере информационных технологий увеличилось на 73,36% и составило 522065 преступлений.

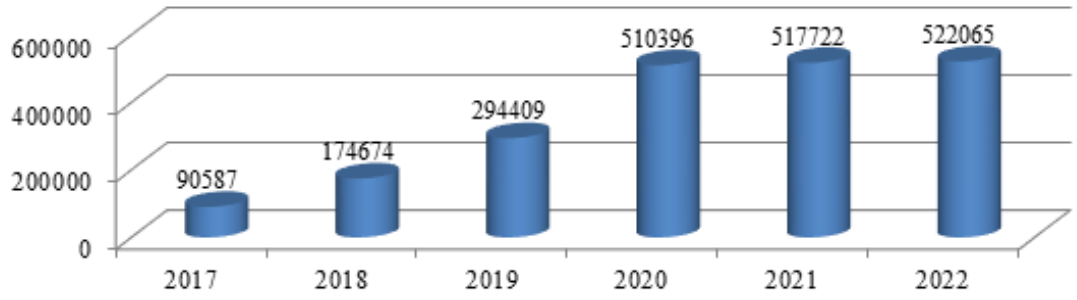


*Рис. 1. Количество официально зарегистрированных преступлений в 2017–2022 гг., совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации*

**Таблица 1**

Динамика количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в Российской федерации в 2018-2022 гг.

| Преступления | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| Всего | 174674 | 294409 | 510396 | 517722 | 522065 |
| Тяжкие | 37949 | 117590 | 222815 | 288312 | 272233 |
| Средней тяжести | 75372 | 97827 | 160823 | - | - |
| Преступлений, совершенных с использованием или применением (пластиковых) карт | 16427 | 34383 | 190167 | 165658 | 127149 |
| Преступлений, совершенных с использованием или применением компьютерной техники | 15027 | 18261 | 28653 | 27519 | 29140 |
| Преступлений, совершенных с использованием или применением программных средств | 4375 | 6283 | 10050 | 7216 | 7649 |
| Преступлений, совершенных с использованием или применением фиктивных электронных платежей | 489 | 984 | 1374 | 954 | 1325 |
| Преступлений, совершенных с использованием или применением сети «Интернет» | 108016 | 157036 | 300337 | 351463 | 381112 |
| Преступлений, совершенных с использованием или применением средств мобильной связи | 61299 | 116154 | 218739 | 217552 | 212963 |

Источник: составлено автором

Отмечается увеличение количества зарегистрированных преступлений на 453,08% совершенных с использованием расчетных (пластиковых) карт (190167); на 56,91% – с использованием компьютерной техники (28653); на 59,96% – с использованием программных средств (10050); на 39,63% – с применением фиктивных электронных платежей (1274); на 91,25% – с применением сети «Интернет» (300337); на 88,32% – с применением средств мобильной связи (218739).

Чтобы проиллюстрировать общие тенденции развития киберпреступности в России, построим график, показывающий количество официально зарегистрированных преступлений в 2017–2022 гг. (рис. 1).

Уровень киберпреступности, т.е. количество преступлений на 100 тыс. населения, в 2022 году также увеличился на 73,4 % с 200,6 в 2021 г. до 347,8 в 2022 г. (рис. 2).

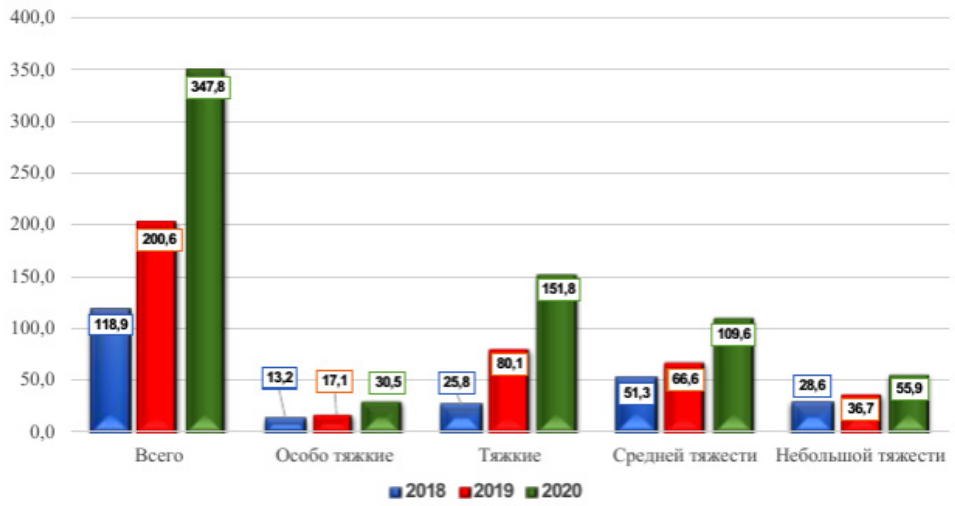


*Рис. 2. Динамика уровня зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в Российской федерации в 2020-2022 гг.*

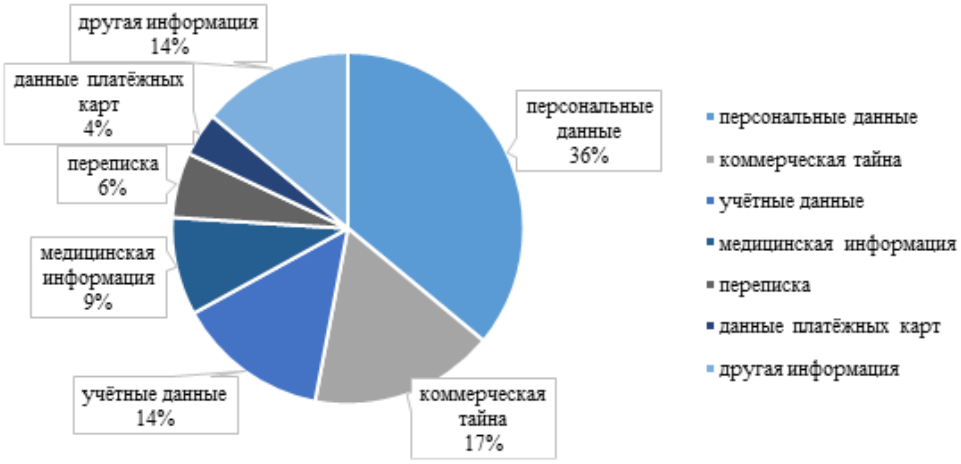


*Рис. 3. Типы украденных данных (в успешных атаках на организации)*

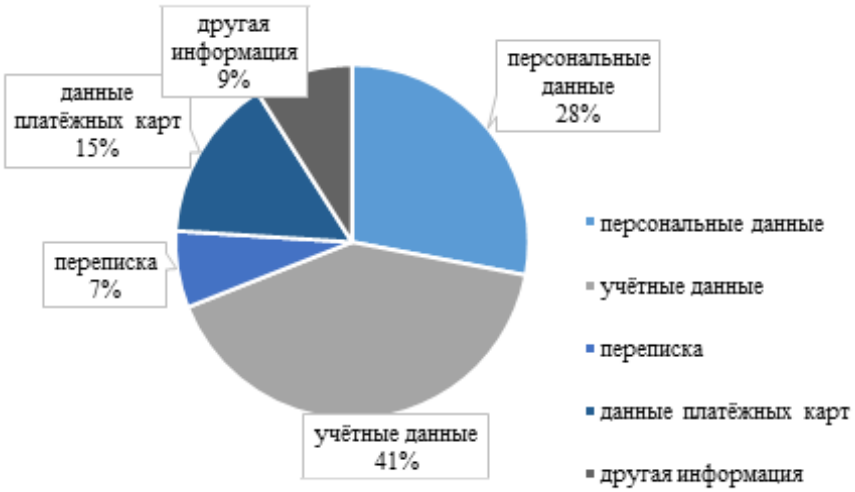


*Рис. 4. Типы украденных данных (в успешных атаках на частных лиц)*


*Рис. 5. Последствия атак на IT-компании (доля успешных атак)*

Что касается структуры преступлений, совершаемых с применением информационно-телекоммуникационных технологий, то среди них преобладают мошенничества (41,24 %), кражи (34,0 %) и деяния в сфере незаконного оборота наркотиков (9,22 %).

Анализируя совокупность факторов, предопределяющих рост киберпреступности, необходимо отметить, что подобная тенденция развития преступности соответствует общемировой. В качестве же основных факторов выделяются:

– доступность информации о способах и средствах совершения киберпреступлений;

– увеличение использования онлайн-коммуникаций как государственными органами, организациями, так и физическими лицами;

– недостаточная цифровая грамотность населения, а также рост пользователей онлайн-сервисов из числа лиц пожилого возраста, которые также не обладают необходимыми знаниями по обеспечению информационной безопасности;

– неподготовленность бизнес-процессов большинства организаций к переводу персонала на дистанционный режим работы;

– рост числа сервисов и объемов онлайн-продаж;

– безработица и желание трудоустроиться на работу с дистанционной занятостью способствуют росту криминальной активности в рассматриваемой сфере и др.

Массовые утечки данных в 2022 году коснулись многих организаций и частных лиц, как в России, так и во всем мире. В нескольких инцидентах пострадали такие известные компании и сервисы, как «Гемотест», «СДЭК», Яндекс. Еда, Delivery Club, DNS [5]. Чаще всего злоумышленники похищали конфиденциальную информацию в медучреждениях (удалось украсть данные в 82% инцидентов), в организациях, занимающихся научными исследованиями или оказывающих образовательные услуги (67%), а также в ритейле (65%).

Злоумышленники скомпрометировали конфиденциальную информацию в 47% успешных атак на организации. Более трети украденной информации (36%) составили персональные данные, также интерес злоумышленников вызывала информация, относящаяся к коммерческой тайне (17%). Учетные данные составили 14% украденных данных. В успешных атаках, направленных на частных лиц, злоумышленникам удавалось украсть данные в 64% случаев. В основном были скомпрометированы учетные данные (41%), а также персональные (28%) и данные платежных карт (15%).

В связи с массовыми утечками данных появляется возможность проведения атак с использованием скомпрометированной информации о пользователях (рис.3, 4).

На протяжении 2022 года количество успешных атак, направленных на IT-компании, постепенно росло, и в IV квартале их число почти вдвое превысило показатели I квартала 2022 года (рис.3). Чаще всего инциденты приводили к утечкам конфиденциальной информации (63%), нарушению основной деятельности (35%), использованию ресурсов компании для проведения атак (13%).

Скомпрометированная конфиденциальная информация в основном включала коммерческую тайну (31%): преимущественно это были многочисленные утечки исходного кода IT-продуктов. Так, в начале года мы наблюдали серию атак группировки Lapsus$, направленную на кражу информации из Globant, Microsoft, Nvidia, Samsung [5]. Скомпрометированные данные впоследствии использовались злоумышленниками, например, украденными сертификатами Nvidia преступники подписывали ВПО, чтобы оно выглядело легитимным.

Решения, предлагаемые IT-компаниями, повсеместно используются другими организациями и частными лицами. Поэтому нарушение деятельности IT-компании может привести к негативным последствиям в отношении клиентов, например, в 46% таких инцидентов у организаций наблюдались сбои в предоставлении сервисов.

Таким образом, киберпреступность создает круг проблем по совершенствованию защитных мер от нелегального доступа к информации в глобальной сети Интернет, использование сведений с целью нанесения вреда с помощью распространения различных программ вирусного характера. Преступления в информационной области привлекают преступников своей значительной выгодностью и неправомерностью преступных действий [6]. В связи с этим в настоящее время крайне необходимо решать проблемы, связанные с киберпреступностью и повышать эффективность способов борьбы.

**Выводы**

Подводя итог всему вышесказанному, резюмируем, что актуальность темы защиты информационной безопасности киберпреступности вызвана тем, что сегодня наблюдаем рост таких явлений, как киберпреступность и кибертерроризм, появляются определенные виды информационного оружия, с помощью которого могут вестись глобальные информационные войны, осложняется решение вопросов сохранения государственной, коммерческой, служебной и персональной тайны, так как низкий уровень отечественных информационных технологий обуславливает построение информационной инфраструктуры России на базе импортной техники и технологий.

Киберпреступность носит трансграничный характер, а Интернет все чаще становится сферой террористических и экстремистских деяний, вовлечения и вербовки молодежи в преступную деятельность, областью целенаправленных кибератак на государственные и коммерческие структуры в преступных целях, включая посягательства на критически важную инфраструктуру, а также дестабилизацию международной информационной безопасности [7]. Использование современных информационно-коммуникационных технологий, без сомнения, выходит за рамки национальной безопасности, так как нуждается в применении действенных механизмов по противодействию угрозам в киберпространстве.

Из анализа стратегий кибербезопасности разных стран видно, что наиболее общим направлением государственной политики является защита стратегических и правительственных информационных систем, таких как информационная система на объектах атомной энергетики, объектах бюджетной и финансовой сферы, государственных банках, в нефтепромышленном и военно-промышленном комплексе. Следовательно, большинство стран, принявших национальные стратегии кибербезопасности, приняли угрозу от киберпреступлений всерьёз, как угрозу национальной безопасности. По нашему мнению, данный аспект также должен быть учтён в принятии стратегии кибербезопасности Российской Федерации.

Основной мерой противодействия в большинстве случаев является правовое регулирование: совершенствование уголовного, административного и информационного законодательства, криминализация новых деяний, ужесточение ответственности за уже существующие компьютерные преступления.

*Библиографический список*

1. Мордвинов К.В., Удавихина У.А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1 (11). С. 83-88.

2. Купирова Ч.Ш., Кузьмин Ю.А. Информационная безопасность как объект киберпреступности // Oeconomia et Jus. 2019. № 4. С. 41-46.

3. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года. [Электронный ресурс]. URL: https://мвд.рф/reports/item/35396677/ (дата обращения 14.10.2023).

4. Простосердов М.А. К вопросу об оценке общественной опасности преступлений, совершаемых в сети Интернет // Актуальные проблемы уголовного права и криминологии: сборник научных трудов кафедры уголовного права. Вып. 3 / Под ред. Ю.Е. Пудовочкина и А.В. Бриллиантова. М.: РАП, 2013. С. 198-209.

5. Актуальные угрозы кибербезопасности: итоги 2022 года. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id1 (дата обращения 14.10.2023).

6. Кириллова А. С. Киберпреступность в Российской Федерации: основные проблемы и способы их решения // Евразийская юридическая конференция: сборник статей Международной научно-практической конференции, Пенза, 23 мая 2018 года / Ответственный редактор Гуляев Герман Юрьевич. Пенза: МЦНС «Наука и Просвещение», 2018. С. 190-193.

7. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1 (53). С. 58-74.