Изварина Н.Ю., доцент кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО «Донской государственный технический университет», Ростов-на-Дону, Россия; nata_don@mail.ru
Охрименко А.Ю., магистрант ФГБОУ ВО «Донской государственный технический университет», г. Ростов-на-Дону, Россия; anjelika1994@mail.ru
Мартиросян А.А., студент ФГБОУ ВО «Донской государственный технический университет», г. Ростов-на-Дону, Россия; Arturo10@yandex.ru

КИБЕРПРЕСТУПЛЕНИЯ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ

Аннотация. Сложность и многогранность киберпреступлений определяет актуальность анализа результатов работы органов внутренних дел Российской Федерации в этой сфере. В статье представлена статистика правоохранительных органов по количеству преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации за 2020 год, проанализирована динамика киберпреступлений в стране по статьям УК РФ за 2018-2020гг.

Ключевые слова: киберпреступления, экономическая безопасность, информационно-телекоммуникационные технологии, компьютерная информация.

Izvarina N. Y., associate Professor of «Economic safety, accounting and law» of the «Donskoy state technical University», Rostov-on-don, Russia; nata_don@mail.ru
Okhrimenko A.Y.,master's student of the «Donskoy state technical University», Rostov-on-don, Russia; anjelika1994@mail.ru
Martirosyan A.A., master's student of the «Donskoy state technical University», Rostov-on-don, Russia; Arturo10@yandex.ru

CYBERCRIME AS A THREAT TO RUSSIA'S ECONOMIC SECURITY

Annotation. The complexity and versatility of cybercrimes determines the relevance of the analysis of the results of the work of the internal affairs bodies of the Russian Federation in this area. The article presents statistics of law enforcement agencies on the number of crimes committed using information and telecommunication technologies or in the field of computer information for 2020, analyzes the dynamics of cybercrimes in the country under the articles of the Criminal Code of the Russian Federation for 2018-2020.

Keywords: cybercrime, economic security, information and telecommunication technologies, computer information.

В реалиях информационно-технологического прогресса преступления в сети интернет играют значительную роль для государства, обусловленную популяризацией IT-технологий во всех сферах жизни общества и, особенно в сфере ведения бизнеса. В современных условиях хозяйствования, при которых делегирование задач на компьютерные и сетевые устройства является нормой, а информационная защита обеспечена многих структур обеспечена не в полной мере, киберпреступники имеют возможность для обогащения. При этом ввиду высокого уровня сложности защиты сетевых данных в мире IT-технологий правоохранительные органы не всегда могут оперативно выявить киберпреступления, они затрагивают не только экономическую сферу страны, но и разрушают её целостность изнутри. Денежные потери в результате действий преступников в киберсфере значительно выше финансового ущерба от других видов противоправной деятельности. Поэтому особую значимость приобретает необходимость выявить слабые места в объектах информационной защиты и усилить контроль там, где могут возникнуть случаи киберпреступлений.

Концепция обеспечения кибербезопасности России подразумевает комплексную защиту объектов безопасности, представленных в таблице 1.

Таблица 1 – Объекты кибербезопасности и применение их в области киберзащиты

Объекты	Применение
Компьютерные сети	Деятельность по защите компьютерных сетей от различных угроз, например, целевых атак или вредоносных программ. Каждая сеть по своей сущности не уникальна и имеет недоработки, через которые злоумышленники могу внедряться и красть данные
Программное обеспечение	Защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках
Информация	Обеспечение целостности и приватности данных, как во время хранения, так и при передаче
Операции в сети	Обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться

Обобщив данные таблицы 1, объектами обеспечения кибербезопасности может выступать любое сетевое оборудование или информационные активы, то есть все устройства, которые имеют доступ в интернет пространство или работоспособность которых зависит от подключения к сети.

Преступления, совершаемые с помощью компьютерных технологий, одни из самых сложных к раскрытию, поэтому наносят значительный ущерб экономической безопасности страны. Раскрываемость данных преступлений на территории Российской Федерации довольно низкая, только пятая часть из них. Информационные преступления с использованием компьютерной техники и программных средств также раскрываются только в трети случаев. Следовательно, детальный анализ таких преступлений, изучение сложных составов будет способствовать повышению эффективности правоохранительных органов в этой сфере.

В 2020 году выявлены преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, связанные со всеми объектами обеспечения кибербезопасности, представленными в таблице 1.Статистика таких преступлений приведена в таблице 2.

Таблица 2– Статистика правоохранительных органов по количеству преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации представлена за 2020 год

Наименование правонарушения	Выявлено		Раскрыто	
	ед.	%	ед.	%
Всего преступлений:	510396	100,0	94942	18,6
в том числе совершенных с использованиемили применением:	267613	52,4	57590	21,5
сети «Интернет»	300337	58,8	56415	18,8
средств мобильной связи	218739	42,9	23969	11,0
расчетных (пластиковых) карт	190167	37,3	32272	17,0
компьютерной техники	28653	5,6	9150	31,9
программных средств	10050	2,0	3595	35,8
фиктивных электронных платежей	1374	0,3	334	24,3
преступления в сфере компьютерной информации, в том числе	4498	0,9	830	18,5
неправомерный доступ к компьютерной информации	4105	0,8	622	15,2
создание, использование и распространение вредоносных компьютерных программ	371	0,1	194	52,3

Согласно данных таблицы 2 на территории Российской Федерации в 2020 году количество совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации составило 510,4 тыс. ед. преступлений. В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5 % в 2019 году до 25,0 % в 2020.Наибольшую долю среди них занимают преступления, осуществленные в сети интернет – 300,3 тыс. ед. преступлений или 58,8 % от общего количества. С использованием средств мобильной связи было проведено 218,7 тыс. ед. преступлений, что составляет 42,9 % от общего количества информационных преступлений. Преступления в сфере компьютерной информации, наиболее значимые и ощутимые с точки зрения финансового эффекта для бизнеса, составили менее 1 % всех информационных преступлений. Неправомерный доступ к компьютерной информации составлял их большую часть. Создание, использование и распространение вредоносных программ повлекло 371 преступление за 2020 год.

Темпы роста информационных преступлений по регионам представлены данными рисунка 1.

Рисунок 1 – Преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации за2020 год на территории РФ

Согласно данных рисунка 1 наибольший темп роста киберпреступлений преступлений отмечен в г. Санкт-Петербург. Наиболее низкие значения этого показателя в Новгородской области.

Преступления, в том числе экономические и особенно совершаемые с помощью компьютерных технологий, одни из самых сложных к раскрытию. Раскрываемость данных преступлений на территории Российской Федерации довольно низкая, только пятая часть из них. При этом информационные преступления с использованием компьютерной техники и программных средств раскрываются более чем в трети случаев. Следовательно, детальный анализ таких преступлений, изучение сложных составов будет способствовать повышению эффективности правоохранительных органов в этой сфере.

Для анализа состояния киберпреступлений в Российской Федерации необходимо использовать структуру преступлений по статьям УК РФ представленную данными таблицы 3.

Таблица 3 – Динамика киберпреступлений в Российской Федерации по статьям УК РФ за 2018-2020гг.

Наименование преступления	Период		
	2018, ед.	2019, ед.	2020, ед.
Предусмотренные гл. 28 УК РФ, в том числе:	3170	3303	3526
Статья 272. Неправомерный доступ к компьютерной информации	1756	1793	1877
Статья 273. Создание, использование и распространение вредоносных компьютерных программ	1409	1504	1643
Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	5	6	6
Статья 159. Мошенничество	6534	7462	7996
Статья 171. Незаконное предпринимательство	1788	1810	1985
Статья 187. Неправомерный оборот средств платежей	315	322	343

Основываясь на данных, представленных в таблице 3, можно отметить, что с 2018 года по 2020 год было выявлено более 30 000 киберпреступлений. Большая часть связанна со ст.159 УК РФ. Данный факт обусловлен постоянным развитием киберкриминала на территории РФ и невозможностью четкого определения каждого уникального киберпреступления в Уголовном Кодексе. В каждом последующем году выявлена положительная динамика роста киберпреступлений в размере 5-10% от числа предыдущего года. За прошедшие 5 лет число выявленных преступлений по каждой статье выросло на 20-50%. Данные таблицы свидетельствуют о перманентном росте киберпреступлений на территории РФ, при том что раскрываемость даже этой малой части выявленных киберпреступлений не превышает 5%.

Повышение роли информационно-коммуникационных технологий отразилось на современных тенденциях киберпреступности: расширяются сферы криминальных интересов, усложняются применяемые преступные схемы. С учетом влияния киберпреступлений на экономическую безопасность страны необходима работа с действующим уголовным законодательством, для формирования достаточной нормативно-правовой базы для охраны соответствующих общественных отношений.

Список литературы

1. Изварина Н.Ю., Климина К.В., Ганжа А.И. Обеспечение финансовой безопасности государства в условиях экономического кризиса // Экономика и бизнес: теория и практика. –2021. – № 6-1 (76). –С. 110-113.

2. Изварина Н.Ю., Шумилина В.Е., Кудовба О.Н. // Статистический анализ преступлений в сфере экономической деятельности Философия права. –2020. –№ 3 (94). –С. 96-104.

3. МВД РФ. – URL:https://мвд.рф/reports/item/22678184/ данные за 2020 год (дата обращения 25.09.2021)

4. Федеральная служба государственной статистики. – URL: http://www.gks.ru/ (дата обращения 25.09.2021).

References

1. Izvarina N.Y., Klimina K.V., Ganzha A.I.Ensuring the financial security of the state in the conditions of economic crisis // Economics and Business: theory and practice. – 2021. – № 6-1 (76). – P. 110-113.
2. Izvarina N.Y., Shumilina V.E., Krutova O.N. //Statistical analysis of crimes in the sphere of economic activity Philosophy of law. – 2020. – № 3 (94). – P. 96-104.
3. The Ministry of Internal Affairs of the Russian Federation. – URL: https://мвд.рф/reports/item/22678184 / data for 2020 (accessed 25.09.2021)
4. Federal State Statistics Service. – URL: http://www.gks.ru / (accessed 25.09.2021).