*Ульяновский государственный университет*

**Артёмова С.Т.***– к.ю.н., доцент*

*кафедры конституционного,*

*административного и гражданского процесса*

*E-mail artemovast@mail.ru*

*Ульяновский государственный университет*

**Клюкина А.В*.*** *– магистрант 2 курса,*

*юридического факультета,*

*Ульяновский государственный университет*

E-mail lady.klyuckina2017@yandex.ru

**КИБЕРПРЕСТУПНОСТЬ - УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ПАНДЕМИИ НОВОЙ КОРОНАВИРУСНОЙ ИНФЕКЦИИ (СОVID-19)**

**Аннотация:** *в статье рассматривается трансформация «традицион­ных» видов преступлений в условиях пандемии новой коронавирусной инфек­ции (COVID-19), выявление актуальности составов преступлений в сфере информацион­ных технологий и связанных с ней ограничений на основании статистики правоохранительных органов. Предложены решения проблем квалификации преступлений с учётом новелл уголовного права на момент про­ведения исследования и анализа особенностей правоприменительной практи­ки и современных тенденций киберпреступности.*

**Ключевые слова:** *IT-технологии,**киберпреступность, информаци­онно-технологический прогресс,**новая коронавирусная инфекция (COVID-19).*

*Ulyanovsk State University*

**Artemova S.T.** *- Candidate of Law,*

*Associate Professor of the Department*

*of Constitutional, Administrative and Civil Procedure*

*E-mail artemovast@mail.ru*

*Ulyanovsk State University*

**Klyukina A.V.** *– 2st year Master's student,*

*Faculty of Law,*

*Ulyanovsk State University*

*E-mail lady.klyuckina2017@yandex.ru*

**CYBERCRIME - IS A THREAT TO INFORMATION SECURITY IN THE CONTEXT OF A PANDEMIC OF A NEW CORONAVIRUS INFECTION (COVID-19)**

**Abstract:** *the article examines the changes in crimes under the conditions of the pandemic of the new coronavirus infection (COVID-19), the identification of the relevance of the elements of crimes in the field of information technology and related restrictions based on law enforcement statistics. Solutions to the problems of crime qualification are proposed, taking into account the novelties of criminal law at the time of the study and analysis of the peculiarities of law enforcement practice and current trends in cybercrime.*

**Keywords:** *IT-technologies, cybercrime, information technology progress, new coronavirus infection (COVID-19).*

Весной 2020 года во всём мире сложилась чрезвычайная ситуация, связанная с появлением новой коронавирусной инфекцией (COVID-19). Указом Президента РФ от 02.04.2020 № 239 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19)»[[1]](#footnote-1) на всей территории Российской Федерации был введен так называемый «режим самоизоляции» принуждающий граждан Российской Федерации находиться в пределах своего дома, чем не смогли не воспользоваться преступники, специализирующиеся на преступлениях в сети Интернет. Сложность обстановки в условии «режима самоизоляции» незамедлительно установила «новые правила игры», а именно обеспечение в условиях карантинных мероприятий, «удалённой работы» многих сфер деятельности: образования, здравоохранения, экономики и государственного управления с использованием элементов искусственного интеллекта, непреднамеренно оказывая влияние на рост компьютерных преступлений и создание благоприятной среды для активизации деятельности преступного сегмента в сфере IT-технологий.

«Новые информационные технологии, в основе которых лежит широкое использование компьютерной техники и средств коммуникаций, оптимизации и автоматизации процессов во всех без исключения сферах жизнедеятельности, привели, вместе с этим, к нивелированию границ и переплетению национальных экономик и национальных инфраструктур стран мира. Более того, указанные тенденции привели к формированию единого мирового информационного пространства, где каждый может получить доступ к любой информации в любой точке планеты, осуществлять дистанционно управление собственными активами и активами компании, заключать хозяйственные договора с иностранными субъектами хозяйствования без необходимости личного контакта и т.д».[[2]](#footnote-2)

«В этих условиях нельзя не согласиться с Россинской Е.Р. и Рядовским И.А., что «лавинообразно возрастающий процесс цифровизации, проникнове­ние современных компьютерных технологий практически во все сферы чело­веческой деятельности: в экономическую, социальную, управленческую, культурную и другие существенно повлиял на жизнь социума, в том числе, не смог не затронуть и судопроизводство, оказав огромное влияние на видоизме­нение преступной деятельности в целом»[[3]](#footnote-3).

«Особенность компьютерных преступлений заключается в том, что в условиях информационно-технологического прогресса они динамично разви­ваются, интегрируя ставшие уже привычными для общества «традиционные» преступления (кражи, вымогательства, шантаж, мошенничество) и совер­шенно новые способы совершения противоправных действий, но мотив кибер­преступников остался прежним: кража денег или информации, которую можно продать, но они приобрели новую «упаковку», адаптированную под ак­туальную повестку дня: продажа поддельных сертификатов о вакцинации в сети Интернет, рассылка SMS-сообщений о штрафах за нарушение режима са­моизоляции и другие. В связи с этим, обеспечение информационной безопас­ности российского общества в условиях массовой цифровизации в Российской Федерации стало еще более актуальным»[[4]](#footnote-4).

«Так, по данным МВД РФ, в 2019 году рост IT-преступности составил 68% по сравнению с 2018 годом – 15% от общего количества преступлений, а в 2020 году только за первые 7 месяцев преступность с использованием IT-технологий выросла на 91,7% по сравнению с аналогичным периодом прошлого года, составив 23% от общего количества преступлений (см. Диаграмму 1.1)»[[5]](#footnote-5).

«Диаграмма 1.1. – «Преступления с использованием IT-технологий в период с 2018-2020 годы»



Подобная динамика объясняется тем, что в период режима самоизоляции трансформация общественной жизни повысила угрозу информационной безопасности граждан и рост компьютерной преступности, поскольку люди, ранее не планирующие осваивать современные цифровые технологии, были вынуждены интегрироваться в новую для них среду общения. Появилось большое число пользователей среднего и старшего поколения, оказавшегося в условиях режима самоизоляции, вынужденных осваивать новые информационные технологии для сохранения связи с миром, сохранения работы и самообеспечения. С учетом малого опыта работы в новой информационной среде, индивидуальных и возрастных факторов, указанные категории пользователей сети стали наиболее уязвимы для манипулирования ими и совершения противоправных действий с их участием.

«Н. Л. Денисов и Н. Ю. Ромашкина определили основные виды совер­шаемых преступных деяний в сфере информационных технологий:

1) совершение противоправного деяния в киберпространстве;

2) использование компьютерных систем или компьютерных сетей, а также иных средств доступа;

3) совершение преступления в рамках компьютерных систем или сетей;

4) направленность деяния против компьютерных сетей, компьютерных систем и компьютерных данных.

Из указанных видов в период распространения новой коронавирусной инфекции (COVID-19) произошел существенный рост преступлений первой группы»[[6]](#footnote-6).

Основные виды таких преступлений:

1. Мошенничество.

Одно из самых актуальных преступных деяний, совершаемые в период распространения пандемии.

С момента начала пандемии было зарегистрировано 1,7 тысячи ложных доменов, содержащих название портала «ГосУслуги»[[7]](#footnote-7), при этом 25% из них были зарегистрированы только за последние семь дней в первой половине апреля. В расчёте на то, что уровень правовой грамотности в Российской Федерации достаточно низкий, злоумышленники рассылают SMS-сообщения с предложением получить социальные выплаты и пособия от государства, при условии перехода по гиперссылке, указанной в SMS-сообщении, заполнить заявление на получение материальной помощи с указанием персональных данных и ввести реквизиты банковской карты, вплоть до СVC-кода[[8]](#footnote-8).

2. Противоправные действия с компьютерной информацией.

«ГСУ СК России по Санкт-Петербургу по поручению Председателя СК России Александра Бастрыкина проведена проверка по факту совершения противоправных действий при проведении дистанционного обучения школьников»[[9]](#footnote-9), по результатам которой возбуждено уголовное дело по признакам преступления, предусмотренного ч. 1 ст. 272 Уголовного кодекса Российской Федерации[[10]](#footnote-10) (далее – УК РФ) (неправомерный доступ к компьютерной информации). К срыву дистанционного обучения школьников может быть причастен пользователь сети «ВКонтакте», позиционируемый себя как «стример» (человек, занимающийся потоковой трансляцией видео в режиме реального времени). На канале «Russia Paver» на платформе YouTube были размещены видеозаписи, на которых блогер присоединялся к обучающим онлайн-трансляциям школьников, с целью сорвать проводимые учебные занятия.

3. Распространение заведомо ложной информации.

«Следственными органами Главного следственного управления Следственного комитета РФ по городу Москве расследовалось уголовное дело, предусмотренное ст. 207.1 УК РФ (публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан). Используя одну из социальных сетей, а также один из видеохостингов киберпреступники распространили под видом достоверной информации видеоролик под названием «гибнут лучшие», и том, что новая коронавирусная инфекция (COVID-19) в действительности не существует. Также в сети размещён видеоролик под названием: «Все больше больных идут на органы», в котором содержится заведомо ложная информация о том, что под видом борьбы с коронавирусной инфекцией производится массовое изъятие у здоровых людей внутренних органов и их последующая продажа для трансплантации»[[11]](#footnote-11).

Ряд отечественных исследователей выделяет основные факторы, определяющие возрастающую с каждым годом международную общественную опасность преступлений в «киберпространстве», а именно:

 1) галопирующую масштабность;

2) возрастающую латентность;

3) невозможность возмещения ущерба;

4) проблему выявления преступников;

5) широкий круг пользователей- распространителей информации.

«Так, по итогам 2022 года глобальная численность пользователей интернета составила более 5,8 млрд. человек. (см. Диаграмму 1.2)»[[12]](#footnote-12).

«Диаграмма 1.2. – «Динамика роста числа интернет-пользователей в период с 2010-2022 годы»



Сложившаяся обстановка в мире осложняется появлением и развитием новейших видов угроз в кибернетической сфере государств, а именно: масштабным распространением «спама»; преступным проникновением на сайты, содержащие, в том числе, личную информацию пользователей; полнейшую бесконтрольность обращаемой информации криминального характера и иное.

Полагаем, что при разработке мер пресечения подобного плана компьютерных преступлений государству необходимо разработать меры профилактического характера по их раннему предупреждению:

1) оптимизировать уголовно-правовые подходы;

2) усилить уголовно-правовую политику;

3) разработать комплекс специальных мер организационно-технического характера в условиях возможных новых всплесков пандемии;

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954 ; Официальный интернет-портал правовой информации http://parvo.gov.ru – 25.03.2022.

2. Указ Президента РФ от 02.04.2020 № 239 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19) // Собрание законодательства РФ. – 2020. – № 14 (часть I). – Ст. 2082 ; Официальный интернет-портал правовой информации http://parvo.gov.ru – 02.04.2020.

3. Бычков В. В. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и общественно значимой информации, повлекшее тяжкие последствия (ст. 207.1, 207.2 УК РФ) : Уголовно-правовая характеристика и сравнительный анализ / В. В. Бычков // Вестник Академии следственного комитета Российской Федерации. – 2020. – № 2(24). – С. 80-84.

4. Веснина С. Н. Модификация киберугроз в условиях сложной эпидемиологической обстановки, вызванной распространением вируса «СOVID-19» / С. Н. Веснина, А. В. Неустроева, К. В. Степанюгин // Гуманитарные, социально-экономические и общественные науки. – Адыгейский государственный университет. – 2020. – № 9. – С. 95-99.

5. Денисов Н. Л. Негативные изменения киберпреступности в период пандемии и пути противодействия им / Л. Н. Денисов // Безопасность бизнеса. – 2020. – № 4. – С. 37-42.

6. Мацько Л. Д. Преступления в сфере информационных технологий в период пандемии COVID-19 / Л. Д. Мацько // Наука молодых – будущее России ; сборник научных статей 5-й Международной научной конференции перспективных разработок молодых ученых: – в 4 томах. – Курск, 10-11 декабря 2020 года. – С. 111-115.

7. Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации / Е. Р. Россинская, И. А. Рядовский // LEX RUSSICA (РУССКИЙ ЗАКОН). – 2019. – № 3. – С. 87-99.

8. Портал государственных услуг Российской Федерации. – Текст : электронный // ГосУслуги : [сайт]. – URL : https://www.gosuslugi.ru (дата обращения : 01.03.2022).

9. Статистика интернета и социальных сетей на 2022 год – цифры и тренды в мире и России. – Текст : электронный // WebСanape : [сайт]. – URL : https://www.wed-canape.ru/business/statustica/html/ (дата обращения : 06.04.2022).

10. Сбербанк предупредил о новых «коронавирусных» схемах мошенников. – Текст : электронный // РИА Новости : [сайт]. – URL : https://ria.ru/20200413/1569941258.html (дата обращения : 28.02.2022).

11. В Санкт-Петербурге возбуждено уголовное дело по факту совершения противоправных действий при прведении дистанционного обучения школьников – Текст : электронный // SLEDCOM : [сайт]. – URL : https://sledcom.ru/news/item/1466453/ (дата обращения : 10.01.2022).

1. Указ Президента РФ от 02.04.2020 № 239 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19) // Собрание законодательства РФ. 2020. № 14 (часть I). Ст. 2082 ; Официальный интернет-портал правовой информации http://parvo.gov.ru 02.04.2020. [↑](#footnote-ref-1)
2. Веснина С. Н. Модификация киберугроз в условиях сложной эпидемиологической обстановки, вызванной распространением вируса «СOVID-19» / С. Н. Веснина, А. В. Неустроева, К. В. Степанюгин // Гуманитарные, социально-экономические и общественные науки. Адыгейский государственный университет. 2020. № 9. С. 96. [↑](#footnote-ref-2)
3. Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации / Е. Р. Россинская, И. А. Рядовский // LEX RUSSICA (РУССКИЙ ЗАКОН). 2019. № 3. С. 87. [↑](#footnote-ref-3)
4. Мацько Л. Д. Преступления в сфере информационных технологий в период пандемии COVID-19 / Л. Д. Мацько // Наука молодых – будущее России ; сборник научных статей 5-й Международной научной конференции перспективных разработок молодых ученых: в 4 томах. Курск, 10-11 декабря 2020 года. С. 113. [↑](#footnote-ref-4)
5. Портал правовой статистики Генеральной прокуратуры Российской Федерации. Текст : электронный // ГенПрокуратура.РФ : [сайт]. URL : https://genroc.gov.ru/stat/data/ (дата обращения : 15.04.2022). [↑](#footnote-ref-5)
6. Денисов Н. Л. Негативные изменения киберпреступности в период пандемии и пути противодействия им / Л. Н. Денисов // Безопасность бизнеса. 2020. № 4. С. 37-42.

Цит. по Ромашкина Н. Ю. Классификация современных киберпреступлений / Н. Ю. Ромашкина, Н. Л. Денисов // Уголовное право и информатизация преступности: проблемы теории, практики и преподавания: материалы Всероссийской научной конференции: сборник научных статей, Москва: Юриспруденция, 2018. С. 254. [↑](#footnote-ref-6)
7. Портал государственных услуг Российской Федерации. Текст : электронный // ГосУслуги : [сайт]. URL : https://www.gosuslugi.ru (дата обращения : 01.03.2022). [↑](#footnote-ref-7)
8. Сбербанк предупредил о новых «коронавирусных» схемах мошенников. Текст : электронный // РИА Новости : [сайт]. URL : https://ria.ru/20200413/1569941258.html (дата обращения : 28.02.2022). [↑](#footnote-ref-8)
9. В Санкт-Петербурге возбуждено уголовное дело по факту совершения противоправных действий при прведении дистанционного обучения школьников Текст : электронный // SLEDCOM : [сайт]. URL : https://sledcom.ru/news/item/1466453/ (дата обращения : 10.01.2022). [↑](#footnote-ref-9)
10. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) // Собрание законодательства РФ. 1996. № 25. Ст. 2954 ; Официальный интернет-портал правовой информации http://parvo.gov.ru 25.03.2022. [↑](#footnote-ref-10)
11. Бычков В. В. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и общественно значимой информации, повлекшее тяжкие последствия (ст. 207.1, 207.2 УК РФ) : Уголовно-правовая характеристика и сравнительный анализ / В. В. Бычков // Вестник Академии следственного комитета Российской Федерации. 2020. № 2 (24). С. 81. [↑](#footnote-ref-11)
12. Статистика интернета и социальных сетей на 2022 год цифры и тренды в мире и России. Текст : электронный // WebСanape : [сайт]. URL : https://www.wed-canape.ru/business/statustica/html/ (дата обращения : 06.04.2022). [↑](#footnote-ref-12)