Секция «Уголовное право и криминология, уголовно-исполнительное право»

Киберпреступность как угроза национальной безопасности Российской Федерации: уголовно-правовая защита граждан Российской Федерации в сфере информационной безопасности

Кутин Павел Максимович
Студент (специалист)
Военный университет Министерства обороны РФ, Москва, Россия
E-mail: pvlfirst@yandex.ru

Кутин Павел Максимович,
курсант 3 курса прокурорско-следственного факультета
ФГКВОУ ВО «Военный университет»
имени князя Александра Невского МО РФ
pvlfirst@yandex.ru
Kutin P.M.,
3rd year cadet of the
Prosecutor's and Investigative Faculty
Military University of the Ministry of Defense of the Russian Federation
pvlfirst@yandex.ru
Наливайко Владимир Олегович
курсант 3 курса прокурорско-следственного факультета
ФГКВОУ ВО «Военный университет»
имени князя Александра Невского МО РФ
mailto:aligarxe@mail.ru

Nalivayko V.O.,
3rd year cadet of the
Prosecutor's and Investigative Faculty
Military University of the Ministry of Defense of the Russian Federation
aligarxe@mail.ru

Научный руководитель:
Сотникова Валерия Владимировна
Старший преподаватель кафедры уголовного права
ФГКВОУ ВО «Военный университет»
имени князя Александра Невского МО РФ, к.ю.н.,
Iris1806@yandex.ru
Supervisor:
Sotnikova Valery Vladimirovna,
candidate of law, Military University of the Ministry
of Defense of the Russian Federation
mailto:Iris1806@yandex.ru

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА ГРАЖДАН РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ CYBERCRIME AS A THREAT TO THE NATIONAL SECURITY OF THE RUSSIAN FEDERATION: CRIMINAL LAW PROTECTION OF CITIZENS OF THE RUSSIAN FEDERATION IN THE FIELD OF INFORMATION

SECURITY Аннотация. В статье рассматриваются вопросы информационной безопасности граждан в Российской Федерации, которые в современных реалиях начали набирать обороты, ведь развивающаяся киберпреступность ставит под угрозу целостность и сохранность государства. В исследовании анализируется статистика преступлений в сфере информационных технологий, а также в статье определены основные проблемы реализации и правоприменения статей Уголовного кодекса Российской Федерации, связанных с преступлениями против собственности, и рассматриваются подходы к улучшению ситуации в сфере информационной безопасности. **Annotation.** The article discusses the issues of information security of citizens in the field of the Russian Federation, which in modern realities have begun to gain momentum, because the developing cybercrime threatens the integrity and safety of the state, analyzes the statistics of crimes in the field of information technology. The article also identifies the main problems of the implementation by the law enforcement officer of articles related to crimes against property, and discusses approaches to improving the situation in the field of information security. **Ключевые слова:** информационная безопасность, киберпреступность, уголовно-правовая защита, мошенничество, персональные данные.

Keywords: information security, cybercrime, criminal defense, fraud, personal data.

В соответствии со статьей 2 Конституции Российской Федерации (далее - РФ) человек, его права и свободы являются высшей ценностью государства[1]. На сегодняшний день тенденции глобализации особенно проявляются в информационной сфере, обеспечивая диалог культур и цивилизаций во всех направлениях жизнедеятельности человечества. Особое место в мире занимают проблемы правового обеспечения информационной безопасности.

Процесс развития технологий обработки, хранения и передачи информации в России приводит к повышенному вниманию к вопросам правового регулирования информационной безопасности, так как играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации. Незаконное и несанкционированное использование информационных ресурсов приводит к серьезным проблемам как у отдельного гражданина, так и у всего государства в целом. Уголовное законодательство направлено на предупреждение и пресечение незаконных преступных посягательств на конституционные права и свободы человека и гражданина.

Преступления в сфере информационных технологий отражены в Уголовном кодексе Российской Федерации (далее - УК РФ)[2]. В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства. Ответственность за совершение указанных преступлений предусмотрена главой 28 Уголовного кодекса Российской Федерации. Постановление Пленума Верховного суда РФ № 48 от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» подробно обозревает правоприменительную практику по квалификации преступлений в информационной сфере[3].

По данным МВД России в период пандемии COVID-19 резко возросло количество преступлений в информационной сфере, а именно деяний, подпадающих под статью 272 УК РФ (неправомерный доступ к компьютерной информации). Активизировалось мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации, так как ограничительные меры, вводимые в связи с пандемией, привели к развитию технологических решений, как например, перевод ряда услуг в онлайн-сферу[4]. Проблема неправомерного доступа к компьютерной информации является одной из самых приоритетных на сегодняшний день в информационную эру, так

как базы данных с номерами и данными граждан РФ попадают к лицам, которые осуществляют свой преступный умысел, используя полученную ими информацию в качестве орудия совершения преступления. База данных номеров граждан РФ незаконно размещается в информационный сети «Интернет», лицо, осуществляющее преступный умысел, использует эти данные для совершения другого преступления, тем самым создают угрозы безопасности граждан РФ.

Уголовная ответственность за данные преступления против конституционных прав граждан РФ крайне мала, что приводит к тому, что лицо, совершающее преступление, между материальной выгодой и риском уголовного наказания выбирает первое. Тем самым совершает преступление, предусмотренное статьей 272 (неправомерный доступ к компьютерной информации) и статьей 159.6 (мошенничество в сфере компьютерной информации), санкцией которого предусмотрен штраф или минимальное лишение свободы.

Согласно статистики, предоставленной МВД России, Генеральной прокуратурой РФ, удельный вес преступлений в сфере IT среди их общего количества увеличился на 5% за пять месяцев[5]. 21 июня МВД опубликовало статистику по преступлениям за январь - май 2021 года. Число преступлений против личности сократилось, но общее количество зарегистрированных преступлений выросло на 1,6% за счет цифровой преступности. В то же время IT-преступность продолжает расти. В январе - мае 2021 года количество таких преступлений выросло на 25,7% в сравнении с аналогичным периодом 2020 года. Увеличивается и доля киберпреступности в общем объеме преступлений - год назад она составлял 21,7%, а сейчас - уже 26,8%, то есть более четверти от их общего количества. В том числе на 48,4% выросло количество преступлений, совершенных при помощи интернета. На 40,1% увеличилось число преступлений с использованием компьютерной техники[6].

В качестве судебной практики служит дело №22-993/2019, которое прошло две судебные инстанции. Гражданин Ербягин А.Е. совершал переводы денежных средств от имени потерпевшей. В следствие чего суд вынес приговор, по которому данный гражданин был осуждён по п. «г» ч.3 ст.158 УК РФ к 2 годам лишения свободы, но суд назначил наказание условным с испытательным сроком 2 года. В свою очередь суд апелляционной инстанции пересмотрев обстоятельства дела, выявил нарушение в части назначения наказания. Поэтому действия Ербягин А.Е. с п. «г» ч.3 ст.158 УК РФ переквалифицировали на п. «в» ч.2 ст.158 УК РФ - кражу, то есть тайное хищение чужого имущества с причинением значительного ущерба гражданину. В итоге по п. «в» ч.2 ст.158 УК РФ Ербягину А.Е. назначено наказание в виде 1 (одного) года исправительных работ с удержанием в доход государства 10% его заработной платы, однако также условно с испытательным сроком 1 год[7].

Данное решение суда свидетельствует о том, что одной из причин растущего количества киберпреступлений в России является чересчур легкое наказание по отношению к лицам, совершающих данную категорию преступлений. Судам необходимо пересмотреть подход к решению данных дел, чтобы небольшое наказание не вызывало чувства безнаказанности.

Тем самым, перед правоприменителем встает проблема правильной квалификации деяния, которое подпадает под два состава преступления. Для решения данной проблемы необходимо более конкретно определить границы преступлений, предусмотренных ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации) и ст.158 УК РФ (Кража). Законодателю необходимо увеличить санкцию по данным составам преступления, так как только решительная уголовная политика государства способна побороть рост киберпреступности.

Резюмируя вышеизложенное, необходимо отметить, что в Российской Федерации ведется активная борьба с киберпреступностью, но ввиду новизны данных преступлений,

отсутствия разъяснений Верховного суда РФ и трудности выявлений и расследования данных общественного опасных деяний виновные лица уходят от уголовного наказания или получают незначительные, часто условные, сроки. Для решения данной проблемы и снижение темпов развития преступлений в информационной сфере необходимо провести соответствующую подготовку правоприменителей, это исключит возможность виновным уйти от справедливого и соразмерного наказания. Так же следует ожесточить ответственность за совершения преступления по ст.159.6 УК РФ (мошенничество в сфере компьютерной информации), так как именно из-за низкого уровня наказания, преступники не боятся совершать данные преступные деяния. Политика информационной безопасности должна иметь многосторонний характер. Ее главными составляющими являются: регулирование информационных отношений в целях обеспечения национальной безопасности, территориальной целостности и общественного порядка, поддержания законности; регулирования информационных отношений в целях обеспечения прав и свобод граждан, здоровья и нравственности; регулирования информационных отношений в сфере коммерческой информации.

Список литературы и источников:

1. Жуков А. З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права // Проблемы экономики и юридической практики. 2019. Т. 15. № 4. С. 141-143.

2. Зюбанов Ю.А. Уголовное право Российской Федерации. Общая часть (в определениях и схемах): учебное пособие. 2-е изд., перераб. и доп. -М.: Проспект, 2019. - Гл.12. - Схемы 84-88. - С. 84-88.

3. Иванов И.Г. Курс уголовного права. Общая часть: учебное пособие- М.: Проспект, 2021. М.: - Гл15. - С. 403-415. - Гл.18,19.

4. Под ред. Бриллиантова А.В. Уголовное право России. Части общая и особенная: Учебник. 3-е издание. - 2021 г.

5. Уголовное право России. Учебник для вузов. Общая часть. Под. ред. А. Н. Игнатова и Ю. А. Красикова. - М.; Издательство НОРМА, 2018. - 639 с.

6. Ульянов М. В. Противодействие преступности в сфере информационно-коммуникационных технологий в условиях применения карантинных мер // Национальная безопасность. 2020. № 2.

[1] Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства РФ. 2020. № 27. Ст. 4196.

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ // Собрание законодательства Российской Федерации. - 1996. - № 25. - Ст. 295

[3] Постановление Пленума Верховного суда Российской Федерации № 48 от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» (с изменениями, внесенными постановлением Пленума ВС РФ от 29 июня 2021 г. № 22) // СПС КонсультантПлюс (дата обращения 20.11.2021)

[4] О состоянии преступности в Российской Федерации в 1-м квартале 2020 года [Электронный ресурс] URL: https://мвд.рф/news/item/19986723/ (дата обращения 24.11.2021)

[5] Состояние преступности в России (форма федерального статистического наблюдения № 4-ЕГС и ведомственного отчета МВД России формы 1-А.) [Электронный ресурс] URL: https://epp.genproc.gov.ru/web/gprf, https://epp.genproc.gov.ru/ (дата обращения 18.11.2021)

[6] МВД России «О состоянии преступности по итогам пяти месяцев 2021 года» [Электронный ресурс] URL: https://мвд.рф/news/item/24738876 (дата обращения 22.11.2021)

[7] Судебное решение [Электронный ресурс] URL: https://sudact.ru/vsrf/doc/?vsrf-txt=&vsrf-case_doc=%E2%84%9622-993%2F2019 (дата обращения 21.11.2021)

Источники и литература

1) 1. Жуков А. З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права // Проблемы экономики и юридической практики. 2019. Т. 15. № 4. С. 141–143. 2. Зюбанов Ю.А. Уголовное право Российской Федерации. Общая часть (в определениях и схемах): учебное пособие. 2-е изд., перераб. и доп. –М.: Проспект, 2019. – Гл.12. – Схемы 84-88. – С. 84-88. 3. Иванов И.Г. Курс уголовного права. Общая часть: учебное пособие- М.: Проспект, 2021. М.: - Гл15. – С. 403-415. – Гл.18,19. 4. Под ред. Бриллиантова А.В. Уголовное право России. Части общая и особенная: Учебник. 3-е издание. – 2021 г. 5. Уголовное право России. Учебник для вузов. Общая часть. Под. ред. А. Н. Игнатова и Ю. А. Красикова. – М.; Издательство НОРМА, 2018. – 639 с. 6. Ульянов М. В. Противодействие преступности в сфере информационно-коммуникационных технологий в условиях применения карантинных мер // Национальная безопасность. 2020. № 2.