Тип работы: Дипломная работа

Предмет: Государственные и муниципальные финансы

Оглавление

ВВЕДЕНИЕ
Компьютерные технологии начинают все активнее интегрироваться в жизнь общества. Современный финансовый рынок уже невозможно представить без их использования, однако это приводит к существенным противоречиям. Увеличивается количество транзакций, способов взаимодействия между субъектами рынка, появляются новые продукты, облегчающие многие отрасли деятельности людей, но при этом постоянно модернизируются виды мошеннических схем и недобросовестных практик, усиливающих негативное влияние на всех участников.
Как отмечается, в Федеральном проекте «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», рост масштабов компьютерной преступности, в том числе международной, выступает одним из вызовов и угроз для реализации целей развития цифровой экономики в сфере информационной безопасности. Действительно, в последние годы отмечается уверенный рост преступлений, совершенных с использованием информационнотелекоммуникационных технологий. Если в 2017 году было зарегистрировано 90 587 таких преступлений [12], то спустя два года, в 2019 году, зарегистрировано уже в три раза больше — 294 409 таких преступлений [12].
За январь — апрель 2020 года преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации зарегистрировано на 82,4 % больше, чем в аналогичный период прошлого года [12]. Во всем мире финансовые институты сталкиваются с различными проблемами, среди которых цифровое мошенничество занимает не самое последнее место. Его уровень растет с каждым годом. По оценкам специалистов главного управления экономической безопасности и противодействия коррупции МВД РФ и Департамента информационных технологий, связи и защиты информации в условиях глобальной пандемии, которая захватила практически все государства мира, число случаев зарегистрированного телефонного и интернет мошенничества выросло на 76% по сравнению с первым полугодием 2019 года.
Интернет все более активно используется для незаконного проникновения в корпоративные и личные базы данных, совершения самых разнообразных мошеннических действий. Компьютерные сети все шире применяются во многих областях жизни российского общества. Столь же быстро растет число

преступлений, связанных с использованием сетевого доступа, множатся способы и формы совершения такого рода деяний. Отчетливо проявляется и тенденция возрастания размера наносимого ими ущерба. По оценкам специалистов МВД, каждый год через Всемирную паутину российские преступники похищают со счетов фирм около 450 млн долл.
Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете [23].
Объектом исследования являются дифференцированные виды мошенничества.
Предмет исследования включает действующее уголовное законодательство России и зарубежных государств, материалы судебно-следственной практики, статистические данные, научные публикации по теме исследования.
Цель исследования – анализ преступлений в сфере мошенничества в сети «Интернет», совершенствование мер государственного управления в сфере государственного противодействия финансовому мошенничеству в сети интернет.
Объектом исследования являются закономерности развития мошенничества в сети «Интернет».
Предмет исследования меры государственного управления в сфере государственного противодействия финансовому мошенничеству в сети интернет.
Обозначенная цель предопределила формулировку и необходимость решения следующих задач:
1. Рассмотреть понятие, признаки финансового мошенничества в сети интернет, причины его распространения.
2. Выделить методы и механизмы совершения финансового мошенничества в сети интернет.
3. Изучить состояние финансового мошенничества в сети интернет в современной России
4. Выделить правовые основы противодействия финансовому мошенничеству в сети интернет и международный опыт противодействия финансовому мошенничеству в сети интернет.
5. Рассмотреть основные проблемы в сфере противодействия финансовому мошенничеству в сети интернет.
6. Предложить пути совершенствования деятельности ОВД в борьбе с финансовым мошенничеством в сети интернет.
Методологической основой исследования является диалектический подход к рассмотрению объекта и предмета исследования. Достоверность исследования достигнута посредством использования системно-структурного, сравнительно-правового, формально-логического и других научных методов.
Теоретическую основу исследования составляют доктринальные источники в области общей теории права, цивилистики, права социального обеспечения, информационного права, банковского права, страхового права, уголовного права, криминологии, экономики. Теоретико-правовым фундаментом работы явились исследования Ф.Н. Багаутдинова, А.И. Бойцова, В.В. Векленко, Б.В. Волженкина, С.М. Кочои, В.Н. Кудрявцева, Н.Ф. Кузнецовой, В.Д. Ларичева, Н.А. Лопашенко, В.В. Мальцева, А.В. Наумова, А.И. Рарога, М.В. Талан, В.С. Устинова и других ученых. Нормативную базу исследования составили Конституция Российской Федерации, международное законодательство, уголовное законодательство России и зарубежных государств, действующее регулятивное законодательство.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ФИНАНСОВОГО МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

1.1 Понятие, признаки финансового мошенничества в сети интернет, причины его распространения

Активное вовлечение России в мировое информационное пространство в начале 1990-х гг. дало мощный толчок развитию коммуникационных технологий, формированию глобальных компьютерных сетей, росту индустрии аппаратного и программного обеспечения, компьютеризации всех сфер экономики и повседневной жизни практически каждого человека. Однако экономическая глобализация и интеграция отдельных государств в единую мировую систему несет в себе как положительный потенциал развития, так и ряд отрицательных факторов. Одним из них, способным негативно влиять на социальную жизнедеятельность, выступает преступность. В современных условиях она превращается в глобальную общечеловеческую проблему [21. С. 91].
Происходит интеллектуализация экономической преступности, которая использует новейшие достижения научно-технического прогресса в своих интересах. Интернет все более активно используется для незаконного проникновения в корпоративные и личные базы данных, совершения самых разнообразных мошеннических действий. Компьютерные сети все шире применяются во многих областях жизни российского общества. Столь же быстро растет число преступлений, связанных с использованием сетевого

доступа, множатся способы и формы совершения такого рода деяний. Отчетливо проявляется и тенденция возрастания размера наносимого ими ущерба. По оценкам специалистов МВД, каждый год через Всемирную паутину российские преступники похищают со счетов фирм около 450 млн долл. [23. С. 7].
Также, по данным официального сайта Главного управления экономической безопасности преступления в сети ив IT сфере занимают второе место от общего числа зарегистрированных правонарушений [33].
Убытки от мошеннической деятельности в Интернете насчитывают каждый год миллионы долларов, увеличиваясь с каждым днем. Данный вид обмана имеет две составляющие: технологическую и психологическую.
Психологическое воздействие на жертву остается прежним. К наиболее распространенным методам мотивации относятся:
- Жажда наживы («гарантированный доход - 201%», «вам полагается компенсация», «вы выиграли в нашем конкурсе»). Относительно новым стала реклама от известных блогеров запрещенных букмекеров и каналов, раздающих деньги. Они предлагают вкладывать средства в раскрутку счета, без каких-либо рисков и со 100% выплатой, т.е. отправляя всего 300 рублей человек должен получить 25000 рублей, однако вернуть назад свои денежные средства еще никому не удалось.
- Страх («ваша карта заблокирована», «срочно оплатите счет», «ваш близкий человек попал в беду»).
- Сентиментальность и жалость (мнимый сбор средств для приюта, помощь людям, попавшим в сложную жизненную ситуацию).
При хищении денежных средств в эпоху всеобщей цифровизации используются различные технологические и коммуникационные возможности компьютерных систем. Одним из наиболее распространенных способов совершения мошенничества является создание злоумышленниками интернет-магазинов. Заказав и оплатив товар люди или вовсе его не получают, или им приходит продукция ненадлежащего качества, несоответствующая описанию. Подобной схемой зачастую пользуются магазины в социальных сетях, таких как ВКонтакте, Одноклассники, Instagram и др. Они соответствуют следующим признакам: реквизитами для оплаты являются номер телефона, личный онлайн-кошелек; отсутствует юридический адрес; стоимость товаров в нем зачастую существенно ниже, чем в других; чрезмерная настойчивость менеджеров. Чтобы избежать разочарования при интернет покупках, следует внимательно изучить сведения о поставщиках, отзывы об организации на сторонних сайтах, не приобретать вещи, имеющие цену намного меньше рыночной.
Для кражи персональных данных (пароля, логина, номера банковской карты, срока ее действия, СУУ-кода) или хищения средств активно используются фишинговые схемы и массовые рассылки почтовых сообщений, содержащих вредоносные программы. Фишинг представляет собой способ введения людей в замешательство посредством получения писем, содержащих различные ссылки, по которым можно попасть на сайт лжесубъектов финансового рынка, имитирующий официальную страницу профессиональных участников.
Для решения представленных задач фишеры применяют следующие методики:
1. Спам-письма. Их идея заключается в запугивании пользователей проблемами, требующих от них немедленной авторизации для выполнения операций (разблокировка счета, отмена ошибочных транзакций). Такой текст направлен на людей с неустойчивой психикой, он достаточно грамотно составлен, но при этом имя жертвы нигде не встречается.
2. Реклама товаров и услуг проверенного интернет-магазина. Этот способ направлен на перевод пользователя на сайт мошенников, которые имитируют платежные сервисы известных площадок. Покупателям предлагают посетить веб-страницу и ввести данные своей карты. Их используют для оплаты онлайн-покупок, вывода средств с помощью системы card-to-card, продажи в DarkNet.
3. Применение вредоносных программ. Мошенники могут присвоить безопасному домену вредоносный IP-адрес, изменив файл, или использовать уязвимость браузера для подключения к нелицензионному сайту.
Для выявления фишинга следует всегда внимательно проверять ссылки, по которым пользователь собирается перейти, защиту соединения перед вводом логина и пароля; по возможности не заходить в личные онлайн-кабинеты через общественный Wi-Fi, т.к. за ним могут стоять мошенники, подменяющие адрес сайта на уровне подключения.
Разновидностью данного вида правонарушений являются массовые звонки на мобильные телефоны граждан от представителей банка - вишинг. Цель мошенников остается прежней - получение личных сведений человека под разными предлогами, стимулирование людей к совершению действий якобы в их собственных интересах. Они достигают ее благодаря множеству ресурсов: информации (у преступников уже есть имя пользователя, адрес, номер телефона, банковские реквизиты), срочность (заставляют

поверить, что деньги жертв находятся в опасности, и действовать нужно быстро), подмена телефона (на дисплее появляется официальный номер банка). Для того чтобы защитить себя от этого вида мошенничества главное помнить, что финансовые работники не станут узнавать номер или CVV-код банковской карты, а также предлагать разрешить какие-либо вопросы без личного присутствия. [16]
В последнее время возросло количество преступных схем, связанных с предложением создания собственного бизнеса в сети Интернет. Потребителю предлагают купить гайд с описанием методики построения предпринимательской деятельности, приносящей достаточно большую прибыль. Полученные от злоумышленников файлы, чаще всего, содержат поверхностную информацию, находящуюся в свободном доступе, или изложение схемы, реализуемой самими правонарушителями.
Очень частым предложением от мошенников является «работа на дому» за хорошее вознаграждение. Как правило, сначала соискателю предлагается выполнить какое-либо легкое тестовое задание, а после перевести небольшую сумму на счет работодателя, объясняя это тем, что жертва подходит на вакантное место, но требуется залог для подтверждения выполнения поставленных задач. После оплаты, безусловно, на связь больше никто не выходит.
Самым кощунственным видом Интернет-мошенничества остаются схемы, связанные со спекуляцией на трагедии. В сети могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт, являющийся копией настоящего, меняю реквизиты для перечисления денег.
Важное значение имеют и организационные причины современной формы финансового мошенничества, к которым можно отнести:
1. Отсутствие эффективной системы обмена информацией о жалобах пользователей.
2. Недостаток постоянного контроля за достоверностью данных, корректностью сведений, рассылаемых по электронной почте, публикуемых в социальных сетях.
3. Несовершенство в работе правоохранительных органов, занимающихся оперативно-розыскной деятельностью.
4. Низкий уровень финансовой грамотности населения.
1.2 Методы и механизмы совершения финансового мошенничества в сети интернет
Механизм совершения мошенничеств в сети интернет, также имеет общие, характерные черты. Ими являются:
1) наличие легенды, в связи с наличием или на осуществление (реализацию) которой требуются финансовые средства, либо необходимо предоставление информации (например, при «фишинге»). Анализ содержания рассылаемых писем, а равно содержания разговоров с потерпевшими позволяет констатировать, что, как правило, виновные применяют дискурсивные/прагматические стратегии: социокультурные формулы приветствия, самоидентификация, формирование доверия потенциального потерпевшего, повествование ему об определенных событиях с целью его побуждения к действию и формированию интереса к благоприятному для него развитию ситуации;
2) использование определенных потребностей или слабостей потерпевших (при «фишинге» - страх потери денежных средств, находящихся на банковской карте; при направлении нигерийских писем - корысть, желание обогатиться; поддельные торговые сайты, либо сайты (агентства) по трудоустройству - потребность в товаре, работе; брачные агентства - желание устроить свою личную жизнь; интернет - попрошайничество - злоупотребление положительными качествами потерпевших, их милосердием и желанием, а иногда и потребностью оказать помощь нуждающимся);
3) обещание достижения потребностей потерпевшего;
4) создание имиджа надежности организации и её маскировка под деятельность легитимных участников рынка.
Считаем, что наличие общих черт в способах и механизмах мошенничеств, совершенных в сети интернет может служить основой для разработки единой методики их раскрытия и расследования.
Мошенничество является одним из преступлений против собственности. Это преступное деяние можно охарактеризовать как одно из наиболее распространенных. Часто преступники в своей деятельности используют ресурсы и возможности Интернета. Рассмотрим некоторые возможные схемы обмана и способы его избежать[17, С.108].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
1. "Конституция Российской Федерации"(принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) Уголовный кодекс Российской Федерации от

13 июня 1996 г № 63-ФЗ // Поправки, внесенные Законом РФ о поправке к Конституции РФ от 14.03.2020 N 1-ФКЗ, вступили в силу 4 июля 2020 года (Указ Президента РФ от 03.07.2020 N 445).
2. Уголовный процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. - 2001.- № 52 (ч. I). - Ст. 4921.
3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. - 2002. - № 1 (часть I). - Ст. 1.
4. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // Собрание законодательства Российской Федерации. - 2017. - № 31 (ч. I).- Ст. 4736.
5. Закон г. Москвы от 19 марта 2008 г. № 14 «О единой системе профилактики правонарушений в городе Москве» [Электронный ресурс]. Доступ из справочной правовой системы «КонсультантПлюс»
6. Багаутдинов Ф.Н. Финансовое мошенничество (уголовно-правовой и криминологический аспекты противодействия) / Ф.Н. Багаутдинов, Л.С. Хафизова. — М. : Юрлитинформ, 2018. — 280 с.
7. Багаутдинов Ф.Н., Хафизова Л.С. Финансовое мошенничество (уголовно-правовой и криминологический аспекты противодействия). М.: Юрлитинформ, 2018. 280 с.
8. Бегишев, И. Р Новый взгляд на мошенничество в сфере компьютерной информации / И. Р. Бегишев // Information Security / Информационная безопасность. - 2016.- № 1.- С. 28-29.
9. Бегишев, И. Р О понятии «электронного средства платежа» в контексте нормы об ответственности за мошенничество, совершенное с его использованием / И. Р. Бегишев // Уголовная политика и культура противодействия преступности: материалы Междунар. науч.-практ. конф., 21 сентября 2018 г.: в 2 т. / редкол.: А. Л. Осипенко, К. В. Вишневецкий, И. А. Паршина, В. С. Соловьев, П. В. Максимов, А. З. Хун. - Краснодар: Краснодарский университет МВД России, 2018. - Т. I.- С. 176-179.
10. Бегишев, И. Р Синдром безопасной атаки: юридико-психологический феномен / И. Р Бегишев // Юридическая психология.- 2018.- № 2.- С. 27-30.
11. Бегишев, И. Р Сравнительно-правовой анализ законодательства Великобритании и России в области противодействия преступлениям в цифровой сфере / И. Р. Бегишев, З. И. Хисамова // Baikal Research Journal. - 2019. - Т. 10. - № 3.
12. Бегишев, И. Р. Безопасность критической информационной инфраструктуры Российской Федерации / И. Р Бегишев // Безопасность бизнеса. - 2019.- № 1.- С. 27-32.
13. Бегишев, И. Р. Криминологические риски применения искусственного интеллекта / И. Р. Бегишев, З. И. Хисамова // Всероссийский криминологический журнал. - 2018. - Т. 12, № 6. - С. 767-775.
14. В Испании задержаны российские Интернет-мошенники. URL: http://www.crimerescarch.ru/news/14.05.2014/234/
15. Гордиенко В. В. Развитие института криминологической и социально-правовой экспертизы: теория и практика // Российский следователь. - 2005. - № 7. - С. 26-31.
16. Данилова, С.И. Особенности и развития профилактики осуществляемой на предварительного расследования, в период // государства и права. - 2017. № 24. С. 35 - 39.
17. Денисов, Н. Л. Концептуальные основы формирования международного стандарта при установлении уголовной ответственности за деяния, связанные с искусственным интеллектом / Н. Л. Денисов //Международное уголовное право и международная юстиция. - 2019. - № 4. - С. 18-20.
18. Денисов, Н. Л. Несоответствие современным реалиям существующей уголовной ответственности за неправомерный доступ к компьютерной информации / Н. Л. Денисов // Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий: сборник материалов межвуз. науч.-практ. конф., 19 апреля 2018 г. - Рязань: Изд-во Рязанского филиала Московского университета МВД России имени В. Я. Кикотя, 2018.- С. 104-107.
19. Денисов, Н. Л., Ромашкина, Н. Ю. Классификация современных киберпреступлений / Н. Л. Денисов, Н. Ю. Ромашкина // Уголовное право и информатизация преступности: проблемы теории, практики и преподавания: сборник статей по материалам Всерос. науч. конф. - М.: Издательский дом «Юриспруденция», 2018. - С. 253-257.
20. Доклад 10 Конгресса ООН по предупреждению преступности и обращению с правонарушителями // 10 Конгресс ООН по предупреждению преступности и обращению с правонарушителями: сборник документов / сост. А.Г. Волеводев. М., 2017.
21. Евдокимов К.Н. Проблемы квалификации и предупреждения компьютерных преступлений. Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2018.
22. Евдокимов, К. Н. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной

информации / К. Н. Евдокимов // Вектор науки ТГУ Серия: Юридические науки. - 2014. - № 4.- С. 33-36.
23. Елин, В.М. Неправомерный к компьютерной информации Бизнесинформатика. 2017. № 2. С. 70 - 76.
24. Ефремова, М.А. Мошенничество с электронной информации // Информационное право. 2017. № 4. С. 19 - 21.
25. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение : дис. ... канд. юрид. наук : 12.00.08 / А. А. Жмыхов. — М., 2013. — 178 с.
26. Законопроект и пояснительная записка разработаны зав. отделом общих проблем криминологии и борьбы с преступностью НИИ проблем укрепления законности и правопорядка при Г енеральной прокуратуре РФ, доктором юридических наук, профессором А. И. Долговой. См.: Проект Федерального закона «О криминологической экспертизе» / Российская криминологическая ассоциация. [сайт]. [Электронный ресурс]. - URL: http://www.crimas.ru/6_3_deyat_zakonotv.php?razdel_zakonotv=proekt_fz_o_krim_expert
27. Исаева Л.М. Правовые основы информационной безопасности : учеб.-метод. материалы. — М. : Моск. ин-т экономики, менеджмента и права, 2018. — 40 с.
28. Краснова, К.А. Правовые и основы предупреждения против участников судопроизводства органами дел // Следователь. 2015. № 22. С. 38 - 41.
29. Лаврентьева Е. «Добро пожаловать, или посторонним вход воспрещен» // «Со-общение»: электронный журнал. [Электронный ресурс]. - 2001. - URL: http://www.soob.ru/n/2001/2/i/12 (дата обращения: 25.05.2009).
30. Магомедов, А.Ш. Просчеты законодателя при реформировании предварительного следствия // Исторические, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2017. № 6(32). С. 118 – 123.
31. Магомедов, Р.Х., Кучинская, Е.Н. Деятельность прокуратуры по защите трудовых прав граждан // Законность. 2017. № 9. С. 41 – 42
32. Малахов А.С. Некоторые особенности раскрытия и расследования мошенничества в сети Интернет / А.С. Малахов, А.С. Дубинин // Актуальные проблемы гуманитарных и естественных наук. — 2017. — № 9. — С. 187-190.
33. Маленкин А.С. Вопросы разграничения мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) и неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности (ч. 2 ст. 272 УК РФ) // Противодействие преступности: от теории к практике день за днем: научно-практическая интернет-конференция Омской юридической академии. Омск, 2016.
34. Махов, В.Н. Роль прокурора в уголовном преследовании в России и зарубежных государствах // Законность. 2014. № 8. С. 32 – 38.
35. Мурадханов, К.Ю. Становление и развитие правового положения прокурора в уголовном судопроизводстве Российской империи // История государства и права. 2014. № 10. С. 47 - 53
36. Неговора, Д.С. Работа органов прокуратуры по противодействию коррупции // Законность. 2016. № 7. С. 16 - 21
37. Нечаева, Е. В. Посягательства на цифровую информацию: современное состояние проблемы / Е. В. Нечаева, Э.Ю. Латыпова, Э. М. Гильманов // Человек: преступление и наказание. - 2019. - Т. 27 (1-4), № 1.- С. 80-86.
38. Никитина И.А. Финансовое мошенничество в сети Интернет / И.А. Никитина // Вестник Томского государственного университета. — 2010. — № 337. — С. 122-124.
39. Номоконов В.А. Глобализация информационных процессов и преступность. URL: http:www.crime-reseach.org/library/nomohon.htm
40. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федеральный закон от 29.11.2017 г. № 207-ФЗ // Российская газета. 2017. 3 дек.
41. О. Ю. Антонов // Вестник Академии Следственного комитета Российской Федерации. - 2017. - № 4 (14). - С. 132-138.
42. Оноколов, Ю.П. Теоретические определения понятий, с предупреждением преступности // Миграционное право. 2011. № 3. С. 23 - 27.
43. Орловский, Е.А., Булатов Р.Б. К вопросу о подготовке кадров прокуратуры Российской Федерации в сфере обеспечения и защиты прав человека // Юридический мир. 2016. № 6. С. 39 - 41.
44. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. М., 2014. 432 с
45. Петроченков, С. Д. Квалификация способов совершения преступления, предусмотренного статьей 183 Уголовного кодекса Российской Федерации / С. Д. Петроченков // Юристъ-Правоведъ. - 2017.- № 1 (80). - С.

59-62.
46. Петроченков, С. Д. Криминологические особенности преступлений в сфере информационно-коммуникационных технологий / С. Д. Петроченков // Вестник Московского университета МВД России. - 2018. - № 6.- С. 155-158.
47. Петроченков, С. Д. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации: законодательный подход и судебная практика / С. Д. Петроченков // Пробелы в российском законодательстве. - 2012.- № 3.- С. 155-157.
48. Поленина С.В. Качество закона и эффективность законодательства. - М., 1993. - С. 43.
49. Правоохранительные и судебные органы России: учебник / В.С. Авдонкин, В.А. Бобренев, О.Н. Диордиева и др.; под ред. Н.А. Петухова, А.С. Мамыкина. М.: Российский государственный университет правосудия, 2015. 434 с.
50. Приходовский М. «Новая концепция развития Интернета в контексте задачи обеспечения информационной безопасности» / «Проза.ру» [Литературный портал]. 20.08.2006. URL: http://www.proza.ru/texts/2006/08/19- 200.html
51. Скрипченко, Н.Ю. Криминологическая личности преступника и развратных действий // Российский следователь. 2016. № 24. С. 45 - 48.
52. Смушкин А. Виртуальные следы в криминалистике / А. Смушкин // Законность. – 2012. – № 8. – 45с.
53. Суворова, Ю.В. Система, принципы и цели административных наказаний // Российская юстиция. 2012. № 12. С. 14.
54. Сургутсков, В.И. Приостановление действия лицензии и аннулирование лицензии как меры обеспечения производства по делам об административных правонарушениях // Современное право. 2018. № 6. С. 14 - 21.
55. Сыдорук, И.И. Государственно-правовое обеспечение правопорядка в Российской Федерации: Монография. М., 2013. 173 с
56. Терюков, Е.О. Проблемы применения временного запрета как меры обеспечения производства по административным делам в области 65 строительства, влекущим наказание в виде административного приостановления деятельности // Актуальные проблемы российского права. 2016. № 11. С. 48 - 53.
57. Хафизова Л.С. Интернет-мошенничество – вопросы уголовной ответственности / Л.С. Хафизова, Ф.Н. Багаутдинов // Правосудие в Татарстане. – Казань, 2017. – № 3 (32). – С. 33–35.
58. Хафизова Л.С. Мошенничество как вид беловоротничковых преступлений по данным Единого учета преступлений в США (UCR – Uniform Crime Reporting in USA) // Социально-правовые проблемы борьбы с преступностью в современной России: Материалы итоговой научно-практической конференции КЮИ МВД России. – Казань: КЮИ МВД России, 2017. – С. 54–56.
59. Хафизова Л.С. Преступления в финансово-экономической сфере: уголовно-правовой и криминологический аспекты // Экономический вестник Республики Татарстан. – 2018. – № 1. – С. 91–94.
60. Хафизова Л.С. Рейдерство, или незаконный захват предприятий, как разновидность финансового мошенничества // Сборник трудов молодых ученых и преподавателей КЮИ МВД России. – Казань: КЮИ МВД России, 2017. – С. 39–43.
61. Хохрин, С.А. Предупреждение пенитенциарной преступности: проблемы и пути решения // Журнал российского права. 2016. № 3. С. 122 - 128.
62. Хренов С. Интернет-мошенничество с использованием технологий сотовой связи. URL: http://www.breru/security/13296/html
63. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2017. № 1. – 22с.
64. Черкашин, А.В. Основные инструменты правового воздействия на общественные отношения в целях предупреждения и раскрытия насильственных преступлений сексуального характера в отношении малолетних // Современное право. 2016. № 6. С. 90 - 95.
65. Шалумов, М.С. Проблемы функционирования российской прокуратуры в условиях формирования демократического правового государства: Дис. на соиск. учен. степ. доктора юрид. наук (12.00.11). Екатеринбург, 2012. 279 с.
66. Шейфер, С.А. Следственная власть: история и современность // Уголовная юстиция. – М.: Актион-Медиа, 2012. – 111 с.
67. Шнайдер Г.Й. Криминология: Пер. с нем./Под общ. ред. и с предисловием Л.О. Иванова - М.: «Про- гресс»-«Универс», 1994. - с. 10-11.
68. Экономическая информатика / под ред. В. П. Косарева, Л. В. Еремина. – М. : Финансы и статистика, 2018. – 592 с.