Юридические исследования
Правильная ссылка на статью:
Ефимовский А.В. — Истоки хактивизма и уголовно-правовое противодействие его проявлениям // Юридические исследования. – 2023. – № 12. – С. 48 - 58. DOI: 10.25136/2409-7136.2023.12.69371 EDN: DVBMBD URL: https://nbpublish.com/library_read_article.php?id=69371

Истоки хактивизма и уголовно-правовое противодействие его проявлениям

Ефимовский Андрей Васильевич

ORCID: 0000-0002-4627-5857

Заместитель начальника научно-исследовательского отдела, Санкт-Петербургский университет МВД России

198206, Россия, г. Санкт-Петербург, ул. Лётчика Пилютова, 1, каб. 406

ave_70@mail.ru

Статья из рубрики "Уголовный закон и правопорядок "

DOI:

10.25136/2409-7136.2023.12.69371

EDN:

DVBMBD

Дата направления статьи в редакцию:

16-12-2023

Дата публикации:

23-12-2023

Аннотация: В статье комплексно рассматриваются вопросы кибербезопасности, а также истоки и принципы хактивизма, даны их определения. Исследуется инструментарий, используемый хактивистами в своей деструктивной деятельности и представлена его классификация. Определяется уголовно-правовая характеристика видов преступлений, используемых хактивистами при осуществлении кибератак. Представлена значимость и необходимость должных мер преодоления явления хактивиза. Анализируются существующие уголовно-правовые методы противодействия проявлениям хактивизма, имеющиеся в российском уголовном законодательстве. Предлагаются меры противодействия IT-угрозам организационного и технического характера. Исследуемая тема требует дальнейшего сбора и обработки эмпирического материала с целью выявления новых методов совершения кибератак на критическую инфраструктуру и

выработки новых подходов к противодействию такого вида преступлениям, обеспечения единообразной практики. В исследовании применяется аксиологический и формально-юридический методы исследования. Эмпирической базой исследования служит анализ специальной литературы по проблеме исследования и статистика о видах и количестве кибератак на информационные ресурсы. Хактивизм является новым явлением в IT-среде. Хактивизм не подразумевает материальную выгоду от совершаемых деяний, что затрудняет его классификацию и разграничение от смежных составов. Таким образом, требуется научное толкование и проработка единого понятийного аппарата для обеспечения единообразной практики выявления и противодействия подобного вида общественно опасным деяниям. В статье делается вывод, что методы, практикуемые хактивистами при проведении кибератак, описаны и имеют свою квалификацию в уголовном законодательстве РФ. Однако, при этом надо учитывать, что часто атаки проводятся с территории других стран и сами группировки являются транснациональными. Следовательно, для успешного противодействия этим деструктивным явлениям необходимо развивать международное сотрудничество в правоохранительной сфере и унифицировать ответственность за подобные деяния. Противодействие хактивизму требует комплексного подхода, включающего юридические, технические и социальные составляющие.

Ключевые слова:

уголовное право, противодействие киберпреступлениям, кибервойна, кибербезопасность, хактивизм, IT-преступления, профилактика преступности, состав преступления, методы противодействия IT-преступлениям, международная преступность

Введение. Информационное пространство пронизывает все сферы жизнедеятельности общества, власти и граждан. Реформа государственного управления требует от органов государственной власти обеспечить переход к информационному обществу путем глубокого внедрения информационных технологий в свою деятельность.

Локдаун, вызванный распространением пандемии COVID-19 привёл к выработке новых форм и методов жизнедеятельности социума в непрерывно развивающейся цифровой среде.

Возможность удаленного получения услуг, предоставляемых государственными организациями, заказа авиа и железнодорожных билетов с электронной регистрацией, банковские онлайн сервисы и т.п. всеми воспринимаются как несомненное благо.

Одновременно с этим растет доля преступлений с использованием IT-технологий. Среди них особое место занимают действия хактивистских группировок.

Материалы и методы. В исследовании применяется аксиологический и формально-юридический методы исследования. Эмпирической базой исследования служит анализ специальной литературы по проблеме исследования и статистика о видах и количестве кибератак на информационные ресурсы.

Целью статьи выступает описание принципов хактивизма, инструментария, используемого хактивистами в своей деструктивной деятельности, и уголовно-правовых методов противодействия данному явлению, имеющихся в российском уголовном законодательстве.

Обсуждение. В настоящее время мировая общественность сталкивается с новыми глобальными вызовами. Прежде всего это передел сфер влияния и крах однополярности в международных отношениях. Однако, при этом постоянное развитие информационного пространства ведет к стиранию границ как в прямом, так и в переносном смысле. Этот тренд несет определенные угрозы и не может не отражаться на столь чувствительной сфере как кибербезопасность.

Как утверждает А.И. Смирнов: «Планета охвачена беспрецедентной информационной революцией. Ее феномен создал условия для формирования глобальной информационной инфраструктуры, которая предоставила принципиально новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям. Однако ИКТ, будучи технологиями двойного назначения, стали не только локомотивом, но и нервом глобализации, ибо несут в себе принципиально новые вызовы и стратегические риски» [1, с. 73].

Среди документов, определяющих подходы к обеспечению информационной безопасности в Российской Федерации, можно выделить:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

- «Основы государственной политики Российской Федерации в области международной информационной безопасности», утверждённые Указом Президента РФ от 12 апреля 2021 г. № 213;

- «Доктрина информационной безопасности Российской Федерации», утверждённая Указом Президента РФ от 5 декабря 2016 г. № 646;

- «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы», утверждённая Указом Президента РФ от 9 мая 2017 г. № 203.

Указанные нормативные правовые акты определяют комплекс требований по обеспечению информационной безопасности для информационных систем. Однако недостаточно полно рассматривают вопросы профилактики и механизмы борьбы с киберугрозами.

Специалисты Лаборатория Касперского под кибербезопасностью позиционируют совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

О.А. Пучков предлагает следующее определение понятия: «Кибербезопасность» – это такой режим охраны данных и информации, который обеспечивает состояние защищенности информации от несанкционированного авторизованного цифрового доступа» [2].

Как видно из определений кибербезопасность пронизывает все сферы человеческой деятельности, связанные с использованием информационных технологий в том числе функционирование органов государственной власти и жизнеобеспечение населения, что является совокупностью взаимно увязанных по времени, ресурсам и месту проведения мероприятий, направленных на создание и поддержание условий минимально необходимых для сохранения жизни и поддержания здоровья людей.

Основную угрозу для киберсистем представляют действия злоумышленников, пытающихся с применением различных технических средств обойти выстроенные системы информационной безопасности. Таких злоумышленников называют хакерами.

Капто А.С. даёт следующее определение: «Хакерами» называют компьютерных злоумышленников, проникающих в государственные и частные информационные банки и добивающихся признания своих технологических способностей. Среди хакеров различают «крэкеров», руководствующихся криминальными интересами, и политически мотивированных «хактивистов» [3].

Специальная военная операция на территории Украины наглядно показала необходимость устойчивой работы электронных ресурсов её обеспечивающих. По данным электронного ресурса «SecurityLab.ru» ещё до начала спецоперации была замечена увеличивающаяся активность хакерских группировок целями которых являлись различные ресурсы Российских министерств, ведомств, государственных корпораций, частных компаний, аффилированных с Российской Федерацией. После начала боевых действий количество атак выросло в геометрической пропорции. Помимо российских ресурсов, атакам подверглись ресурсы иностранных компаний, отказавшихся уйти с российского рынка. Можно констатировать факт, что 25 февраля 2022 года было положено начало настоящей кибервойне, в которую, помимо прочих, вступили хактвисты группировки Anonymous.

По мнению Капто А.С.: «Кибервойна – один из новых видов войны, основанный на современных технологиях. Это не самостоятельный вид противоборства, кибервойна всегда является составной частью информационной войны, и в целом выступает элементом полномасштабной военной кампании, включающей как недавно возникшие, так и более привычные способы борьбы» [3].

Можно проследить хронологию событий. 26 февраля 2022 года зафиксировано более 50 DDoS-атак мощностью более 1 Тбайт, а также ряд профессиональных целевых атак на портал Госуслуг. О трудностях с доступом на сайт сообщал также «Первый канал», причиной сбоя его представитель назвал DDos-атаки. Госкорпорация «Роскосмос» заявила, что ее сайт также подвергся DDoS-атаке из-за рубежа. С такой же проблемой столкнулись «Российские железные дороги».

Не осталась в стороне от начавшейся кибервойны и российская хактивистская группировка Killnet, в свою очередь, атаковавшая сайт группировки Anonymous.

Вот небольшое перечисление активности группировки Killnet:

15 апреля 2022 года – атаки на Министерство обороны ФРГ https://www.bmvg.de/ (остановлена спустя 5 часов), международный аэропорт Кёльн/Бонн (ФРГ) http://www.koeln-bonn-airport.de/ (остановлена спустя 14 часов);

16 апреля 2022 года – атаки на аэропорт Гатвик (Великобритания) https://www.gatwickairport.com/ (остановлена спустя 5 часов), ООН https://www.un.org/ (остановлена спустя 5 часов), ОБСЕ https://www.osce.org (остановлена спустя 4 часа), немецкий банк «Commerzbank» https://www.commerzbank.de/ (остановлена спустя 1 час), немецкий банк «KFW» https://www.kfw.de/ (остановлена спустя 4 часа);

21 апреля 2022 года – атака на Кибер-Центр НАТО https://ccdcoe.org/ (остановлена спустя 3 часа).

Также за короткий промежуток времени группировкой Killnet были осуществлены атаки на сетевые инфраструктуры Украины, Польши Чехии, Румынии, Молдавии, Эстонии, Латвии и Литвы. 1-3 мая 2022 года была проведена повторная массированная атака на сетевую инфраструктуру ФРГ. Целями атак являлись информационные ресурсы и сетевые коммуникации органов государственной власти, авиаперевозок, железнодорожного сообщения, банковских структур, порталов государственных услуг.

13 апреля 2022 года Killnet объявили о создании «Международного Альянса Хактивистов». В своём меморандуме Международный Альянс Хактивистов[1] заявляет следующие цели своего создания: уничтожение фашизма в интернете; предотвращение расширения НАТО, в том числе посредством уничтожения части инфраструктуры в ходе хакерских атак; уничтожение интернет-ресурсов террористических группировок, в том числе сайтов для вербовки наемников и официальных аккаунтов в мессенджерах и соцсетях; создание единого центра мониторинга для обеспечения безопасности в интернете с помощью новых технологий. В первую очередь центр будет собирать данные о неонацистских сектах, после чего по ним будут нанесены удары и применение к ним соответствующей силы); создание в дружественных странах 60 интернет-представительств, которые обеспечат коммуникации с населением этих государств; оказание помощи жертвам мошенничества в интернете через специальный благотворительный фонд.

Хактивисты группировки Anonymous в апреле 2022 года также провели ряд атак против информационно-сетевых ресурсов Российской Федерации и Республики Беларусь. Прежде всего выделяются атаки на сетевые ресурсы аэропортов и железных дорог, что затрудняет перевозки и приводит к срыву логистических цепочек. Под удар попали и банковские структуры, что также ведет к срыву платежей и как итог срыву поставок.

Anonymous атаковали: энергетическую организацию «Электроцентромонтаж», которая занимается проектированием, испытаниями, строительством, монтажом и обслуживанием электротехнического оборудования объектов генерации и передачи электроэнергии в России; ПСКБ «Петербургский социальный коммерческий банк», входящий в число крупнейших российских банков по размеру активов; таможенного брокера для компаний топливно-энергетического комплекса «АЛЭТ», осуществляющим экспорт и таможенное оформление энергитических ресурсов (угль, сырая нефть, углеводородные продукты и продукты переработки нефти). В обращение были выложены более 6 ТБ данных через некоммерческий сайт Distributed Denial of Secrets (DDoSecrets), публикующий различные утечки.

И.Н. Панарин в монографии «Информационная война и выборы» обозначил «хактивизм» как «бескорыстное» хакерство в целях политического активизма [4, с. 345].

Однако, «Хактивизм» это не обязательно «бескорыстное» хакерство, мы скорее считаем, что «хактивизм» это хакерство в политических и военных целях. Тем более, что политически ангажированные хакеры все чаще стоят на службе у властных и политических структур получая не только идеологическую поддержку, но и материальное стимулирование [5].

Хактивистские кампании нацелены на достижение политической, социальной или религиозной справедливости в соответствии с целями группы. Термин «хактивизм» впервые был использован в 1996 году хакером под ником Omega, являвшимся членом организации Cult of the Dead Cow.

Хактивизм анонимен, хактвистские группы работают, редко раскрывая своих членов.

Из определения хактвизма видно, что цели, преследуемые хактвистами вполне благие. Однако методы, которыми достигаются эти цели далеки от идеала. Атаки на некоторые цифровые ресурсы могут привести к затруднениям в жизнеобеспечении населения, а порой и к угрозе возникновения чрезвычайных ситуаций.

За время существования хактвисты провели ряд успешных операций, самыми нашумевшими среди них были следующие:

1. Anonymous в течение многих лет не проводил атак. О группировке вновь заговорили в 2020 году, после смерти Джорджа Флойда. Она резко выступила против полицейского произвола в поддержку общественно-политического движения Black Lives Matter (BLM) в Twitter. Группировка провела ряд DDoS-атак, которые на короткое время обрушили официальный сайт Департамента полиции Миннеаполиса и правительственный сайт города Баффало в штате Нью-Йорк, США.

2. Сирийская электронная армия (SEA), проводила операции с использованием фишинга и DDoS-атак, чтобы взломать сайты ряда правительственных структур США, частных компаний и крупнейших медиа-групп. Хактвистская группа успешно опубликовала в Twitter ложный твит о взрыве в Белом доме и ранении президента США, в результате чего индекс Доу-Джонса упал на 140 пунктов.

3. В 2016 году группа WikiLeaks, созданная Джулианом Ассанжем, выложила в общий доступ электронные письма от Демократического национального комитета. Утечка электронных писем повлияла на предвыборную кампанию Хиллари Клинтон и многие стала причиной ее проигрыша на президентских выборах.

4. Хактвисты группировки Worms Against Nuclear Killers (W.A.N.K.) на волне антиядерных протестов внедрили два червя W.A.N.K и OILZ в компьютерную сеть DECnet, принадлежащую Национальному американскому космическому агентству NASA. Черви препятствовали доступу к учетным записям сети и файлам и проводили смену паролей.

Можно выделить четыре типа хактивизма:

- политический – имеет задачей оказать влияние на население при достижении определенных политических целей;

- социальный – направлен на то, чтобы вызвать социальные изменения в обществе;

- религиозный – может иметь целью как на вербовку в религиозную организацию, так и разрушение религиозной организации;

- анархический – цели могут иметь анархистскую повестку разрушения гражданской или военной инфраструктуры какого-либо государства в целом.

Мишенью хактивистов обычно становятся крупные организации, государственные структуры, публичные лица, чьи действия противоречат идеологии хактивистов. Например, атака может быть направлена против организации, которая, по мнению хактивистов, нарушает права человека или свободу распространения информации. Эксперты, атакующие организации с целью привлечь внимание общественности к уязвимостям, также могут считаться хактивистами.

Рассмотрим методы, которые хактвисты используют для достижения своих целей. Они используют те же методы, что и обычные киберпреступники. К самым распространенным

из них относятся:

- DDoS-атаки – атаки, проводимые с множества устройств одновременно, чтобы сделать тот или иной ресурс недоступным для пользователей;

- Дефейс — изменение содержимого сайта, подвергнутого атаке. Как правило на взломанных сайтах публикуются прокламации, продвигающие идеи атаковавшей группировки;

- Доксинг — сбор конфиденциальной информации о человеке или организации с целью дальнейшего её обнародования в инфопространстве;

- SQL-инъекция – завладение информацией из баз данных, путем использования уязвимостей в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL);

- Фишинг – атака, целью которой является получение обманным путём конфиденциальной информации пользователя (пароли, данные банковских карт и т.д.).

Теперь перейдем к квалификации вышеперечисленных действий.

Под DoS-атакой понимается атака на вычислительную систему с целью довести её до отказа, путём создания таких условий, когда пользователи лишены возможности получить доступ к запрашиваемым электронным ресурсам, либо этот доступ становится для них затруднённым [6]. «DoS» - «Denial of Service» – означает «отказ в обслуживании».

DDoS-атака «Distributed Denial of Service» – означает «распределённый отказ в обслуживании» и проводится в отношении серверов с хорошо выстроенной защитой, что требует большего количества, участвующих в атаке, устройств.

Результатом DDoS-атаки могут быть: отказ в обслуживании части пользовательских запросов; существенное замедление времени ответа на запросы к атакованному серверу; прикрытие несанкционированной активности на атакованном web-ресурсе.

Надо учитывать, что блокировка доступа к серверам, отвечающим за работу интернет ресурсов и баз данных, может приводить к тяжким последствиям или создавать угрозу их наступления. Замедление или полная блокировка доступа к системам, отвечающим за работу аэропортов или движение составов на железных дорогах, мониторинговым системам атомных электростанций и т.п. может повлечь возникновение техногенных катастроф и привести к гибели людей и крупному материальному ущербу.

DDoS-атаки квалифицируются по общим нормам о преступлениях в сфере компьютерной информации: ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» и ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Максимальная санкция за совершение такого рода действий до семи лет лишения свободы.

Доксинг. Первым случаем доксинга можно считать создание Нилом Хорсли веб-сайта под названием «Нюрнбергские файлы». На этом ресурсе были размещены личные данные примерно 200 человек, осуществлявших операции по искусственному прерыванию беременности. Медицинская организация «Planned Parenthood» обратилась с иском о запрете на распространение данной информации и блокировки сайта. В 2002 г. иск был удовлетворен Апелляционным судом 9-го округа США [6].

Следует учесть, что в случае хактивистской атаки с применением доксинга полученная информация используется не с целью обогащения или шантажа, а для придания огласке принадлежности к определенным властным и социальным группам. В подавляющем большинстве случаев систематизированная информация придается огласке, что в сопровождении с какими-то обвинениями наносит серьезный вред [6].

Доксинг можно квалифицировать по ст. 137 УК РФ. «Нарушение неприкосновенности частной жизни» Максимальная санкция по данному составу - лишение свободы на срок до двух лет.

SQL-инъекция позволяет атакующему использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для манипулирования базой данных и получения доступа к потенциально ценной информации. Атаки на основе таких уязвимостей – одни из самых распространенных и опасных: они могут быть нацелены на любое веб-приложение или веб-сайт, которые взаимодействуют с базой данных SQL (а подавляющее большинство баз данных реализованы именно на SQL).

SQL-инъекция может привести к следующим последствиям: раскрытие конфиденциальных данных; компрометация целостности данных; нарушение приватности пользователей; неправомерное получение административного доступа к системе; неправомерное получение общих прав доступа к системе.

SQL-инъекция является преступлением, квалифицирующимся по ст. 272 УК РФ «Незаконный доступ к компьютерной информации». Также в данном случае применимы ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», ст. 285.1 УК РФ «Нарушение правил функционирования информационной системы или сети Интернет» и ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации».

Фишинг (от англ. phishing, происходит от fishing – рыбная ловля, выуживание) является одним из наиболее распространенных методов совершения мошенничества в киберпространстве, который используется для хищения паролей и конфиденциальной информации путем введения клиента в заблуждение [7].

По методу воздействия фишинг можно классифицировать на два типа:

Фейковый сайт – используется тот же интерфейс, что у оригинала сайта, подбираются похожие домены, что вводит пользователей в заблуждение. В адресе может быть изменен один знак, например, английская строчная L и заглавная I. https://www.uralsib.ru/ и https://www.uraIsib.ru/ разные домены, хотя визуально не отличаются;

Вредоносный файл – как правило, это архив, при открытии которого гаджет или устройство заражается вирусом, который шпионит за жертвой, собирает данные и отправлять на устройства злоумышленникам.

Фишинг по своей сути является мошенничеством в цифровой среде, можно при квалификации данного вида действий использовать постановление Пленума Верховного Суда РФ № 51 от 27 декабря 2007 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» разъясняет, что в случаях, когда указанные деяния сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-

вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по ст. 159 УК РФ, а также, в зависимости от обстоятельств дела, по ст. ст. 272 или 273 УК РФ.

Таким образом можно выделить группу преступлений, в которых объектом преступных действий является компьютерная информация, к ним относятся DDoS-атаки, SQL-инъекция и Фишинг. Исходя из деления по объекту и субъекту преступления, предметом этой группы преступлений выступает сама компьютерная информация, что вытекает из сути противоправных деяний, установленных в ст. 272, 273 УК РФ.

Рассмотрим вопрос противодействия хактивизму. Всеобщая цифровизация постепенно стирает границы и создает общее цифровое пространство, что влечет возникновение определенных сложностей в выработке мер противодействия хактивизму. Хактивистские группировки формируются не по национальному, а по идеологическому принципу, следовательно, атаки могут проводится одновременно с IP-адресов имеющих различную юрисдикцию.

Следует отметить, что с началом специальной военной операции на Украине контакты в правоохранительной сфере практически заморожены. Усиление поляризации на международном уровне препятствует эффективному сотрудничеству, и киберпространство все чаще используется в политических и идеологических целях [8].

Киберпреступность также имеет ярко выраженную трансграничность, таким образом, меры противодействия хактивизму будут также иметь схожий характер. Меры противодействия можно разделить на организационные и технические.

К организационным мерам можно отнести:

1. Развитие международного сотрудничества правоохранительных органов в процессе предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием IT-технологий;

2. Создание международных институтов, отвечающих за вопросы унификации законодательства в области противодействия преступлениям, совершаемым с использованием IT-технологий;

3. Совершенствование законодательства регулирующего правоотношения в IT-среде;

4. Подготовка высококвалифицированных IT-специалистов для правоохранительных органов;

5. Повышение компьютерной грамотности населения и должностных лиц.

К техническим мерам можно отнести:

1. Усиление требований, предъявляемых к разработке систем в целях недопущения утечки сведений закрытого характера в открытый доступ;

2. Совершенствование систем защиты каналов передачи данных и баз данных от несанкционированного доступа;

3. Повышение технической оснащенности органов государственной власти и силовых структур;

4. Разработка национальных программных продуктов, в том числе операционных систем;

5. Повышение «живучести» информационных систем жизнеобеспечения и каналов связи;

6. Дублирование критически важных информационных систем.

Вывод. Подводя итоги можно сказать, что методы, практикуемые хактивистами при проведении кибератак, описаны и имеют свою квалификацию в уголовном законодательстве РФ. Однако, при этом надо учитывать, что часто атаки проводятся с территории других стран и сами группировки являются транснациональными. Следовательно, для успешного противодействия этим деструктивным явлениям необходимо развивать международное сотрудничество в правоохранительной сфере и унифицировать ответственность за подобные деяния. Противодействие хактивизму требует комплексного подхода, включающего юридические, технические и социальные составляющие.

Библиография

1. Смирнов А. И., Григорьев В. Р., Кохтюлина И. Н., Куроедов Б. В., Сандаров О. В. Глобальная безопасность в цифровую эпоху: стратагемы для России / А. И. Смирнов, В. Р. Григорьев, И. Н. Кохтюлина Б. В. Куроедов, О. В. Сандаров. – Москва : Государственный научный центр Российской Федерации Всероссийский научно-исследовательский институт геологических, геофизических и геохимических систем, 2014. – 394 с.
2. Пучков О. А. Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике // Право и государство: теория и практика. – 2019. – №5 (173). – С. 66-69.
3. Капто А. С. Кибервойна: генезис и доктринальные очертания // Вестник Российской академии наук. 2013. Т. 83. № 7. С. 616.
4. Панарин, И. Н. Информационная война и выборы / И. Н. Панарин ; И. Н. Панарин. – Москва : Городец, 2003. – 411 с.
5. Акопов, Г. Л. Хактивизм – угроза информационной безопасности в информационном социуме / Г. Л. Акопов // Государственное и муниципальное управление. Ученые записки СКАГС. – 2015. – № 3. – С. 195-199.
6. Романовская Е. А. «Публично-правовые основы противодействия доксингу» Электронный научный журнал «Наука. Общество. Государство». 2023. Т. 11, № 2. С. 70.
7. Vincent A. Don’t feed the phish: how to avoid phishing attacks. Network Security. 2019; 2:11–14.
8. Яковлева, А. В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) / А. В. Яковлева // Социально-политические науки. – 2021. – Т. 11, № 4. – С. 70-81.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Представленная на рецензирование научная статья на тему: «Истоки хактивизма и

уголовно-правовое противодействие его проявлениям» представляет собой актуальное исследование, которое можно было бы охарактеризовать в качестве междисциплинарного, так как объективно находится в плоскости политологической и правовой одновременно. Актуальность проведенного исследования обоснована увеличением количества информационных противодействий, кибератак в отношении органов государственной власти и управления в Российской Федерации, объектов критической инфраструктуры после начала СВО, де-факто в глобальном масштабе, невиданном ранее. Произошел резкий рост преступлений с использованием IT-технологий, среди которых авторами особенным образом выделены именно действия хактивистских группировок.

Авторами определен предмет исследования, определена его цель и задачи. Исследование обладает определенной научной новизной, несмотря на то обстоятельство, что данная проблема находится в центре внимания современных ученых-исследователей и, все более и более, в рамках отдельных отраслей права.

Положительно следует отметить, что рецензируемая статья структурирована и в ней выделен специальным образом методологический раздел. Использованы различные методы и подходы. Анализ источниковой базы исследования показал, что при подготовке рецензируемой статьи было использовано достаточное скромное количество научных работ (8 позиций) разных лет. К сожалению, данное обстоятельство, по нашему мнению не позволило авторам развернуть полноценную научную дискуссию.

Содержательно в статье проанализированы основные понятия, связанные с информационной и кибербезопасностью. Представлена группа основных нормативных правовых актов, документов концептуального и стратегического характера, определяющих комплекс требований по обеспечению информационной безопасности в Российской Федерации. Сделан авторский вывод о недостаточности содержащихся в них превентивных, профилактических мер и механизмов борьбы с киберугрозами.

Приведены многочисленные примеры противоправных действий зарубежных хакерских организаций, в частности, перечислены активности группировки Killnet, что делает статью достаточно увлекательной в плане ее прочтения и использования в научной и научно-просветительской деятельности по проблемам кибербезопасности. Выделена группа преступлений, в которых объектом преступных действий является компьютерная информация, а, также, меры противодействия – технические и организационные.

Отдельно следует указать на то обстоятельство, что, представленная на рецензирование научная статья «Истоки хактивизма и уголовно-правовое противодействие его проявлениям» не вычитана авторами тщательно. В нескольких предложениях содержаться недочеты, связанные с банальными грамматическими ошибками, неправильным предложным согласованием. Тем не менее, сказанное не влияет на качество статьи в целом.

Таким образом, исходя из вышеизложенного, считаем, что рецензируемая научная статья на тему: «Истоки хактивизма и уголовно-правовое противодействие его проявлениям» соответствует необходимым требованиям, предъявляемым к такому виду научных работ и ее можно рекомендовать к опубликованию в искомом научном журнале.