УДК 32 **DOI: 10.34670/AR.2024.17.66.008**

Влияние роста киберпреступности на общемировую экономическую безопасность

Майстренко Григорий Александрович

Кандидат юридических наук, старший научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
e-mail: G.Maystrenko@yandex.ru

Аннотация

Статья посвящена актуальной на сегодняшний день проблеме роста киберпреступлений и их влиянии на экономическую безопасность во всем мире. Изучены понятия хакерства и онлайн-мошенничества, приносящие огромную долю прибыли организованной преступности в большинстве развитых стран. В качестве исследовательской задачи можно обозначить оценку рисков возрастающей киберпреступной деятельности в различных областях современного общества. В настоящей работе предпринимается попытка создать концептуальную модель, анализирующую киберпреступность в контексте влияния на общемировые социально-экономические показатели, в качестве основных аналитических инструментов используется набор социальных, экономических, политических и технологических показателей кибербезопасности. Авторы приходят к выводу, что киберпреступления оказывают пагубное воздействие на жизнь, экономику и международную репутацию стран, в этой связи борьба с киберпреступностью требует комплексного подхода.

Для цитирования в научных исследованиях

Майстренко Г.А. Влияние роста киберпреступности на общемировую экономическую безопасность // Теории и проблемы политических исследований. 2023. Том 12. № 10А. С. 59-64. DOI: 10.34670/AR.2024.17.66.008

Ключевые слова

Киберпреступность, Интернет, хакерство, кибербезопасность, онлайн-мошенничество, организованная преступность.

Введение

Основной и движущей силой глобализации является научный прорыв в области информационных и коммуникационных технологий, а динамические изменения во всех аспектах человеческого существования являются основным побочным продуктом нынешнего периода глобализации цифровой революции.

Мы можем наблюдать, как новейшие разработки в области информационных технологий предоставляют развивающимся странам исключительные возможности для реформирования систем образования, более эффективной разработки и реализации политики, а также расширения диапазона перспектив для бизнеса.

Бесспорно, весь мир постепенно «оцифровывается», а глобализация расширяется с каждым днем благодаря бесперебойным и высокофункциональным информационным и коммуникационным технологиям. При этом глобализация, помимо очевидных преимуществ, несет и негативные последствия, такие, как киберпреступность и киберугрозы. А особенность интернет-пространства заключается в том, что преступная деятельность в виртуальном мире предоставляет преступникам более широкий диапазон для различных махинаций.

Основное содержание

Социальные и экономические факторы отражают уровень регионального развития и служат фундаментальным контекстом возникновения киберпреступности. Учитывая присущую киберпреступности технологическую природу, глобальная урбанизация и революция в области информационных технологий способствовали развитию глобальной связи и создали беспрецедентные условия и возможности для киберугроз.

С другой стороны, экономически развитые регионы обычно имеют отличную инфраструктуру информационных технологий, которая может предоставить киберпреступникам удобные и доступные условия для совершения преступлений. Высокий уровень образования также, вероятно, взаимосвязан с киберпреступностью, поскольку киберпреступность обычно требует определенного уровня компьютерных навыков и знаний в области информационных технологий. То, что социально-экономические условия связаны с большей активностью киберпреступников, говорит о том, что социальный и экономический фактор непосредственно связан с ростом киберпреступности.

Влияние политических факторов на киберпреступность в основном отражается в регулировании и мерах правительства по предотвращению и контролю киберпреступности, таких как построение грамотной правовой системы и непосредственный контроль на государственном уровне.

Как и в случае с традиционными преступлениями, отсутствие эффективного механизма социального контроля и наказания будет способствовать развитию преступного поведения. Сдерживающий эффект законодательства заставляет киберпреступников задуматься о последствиях, которые им придется нести. Хотя виртуальный и транснациональный характер киберпространства позволяет преступникам избежать наказания, киберпреступность можно в некоторой степени сдержать за счет повышения строгости наказания и международного сотрудничества правоохранительных органов [Сухаренко, 2009, с. 30].

С другой стороны, киберпреступники могут искать защиту через коррупционные связи с местной институциональной средой, что ослабит деятельность правоохранительных органов и будет способствовать киберпреступной деятельности. Например, коррупция в

правоохранительных органах затрудняет наказание киберпреступников, а коррупция среди сетевых операторов или интернет-провайдеров облегчает киберпреступникам подачу заявок на вредоносные доменные имена или регистрацию поддельных веб-сайтов. Некоторые исследования показали, что в регионах с высоким уровнем коррупции обычно наблюдается больше киберпреступной деятельности. Итак, киберпреступления обычно объясняются политической коррупцией, неэффективным управлением, институциональной слабостью и слабым верховенством закона [Аникьева, Дегтерева, 2020, с. 14].

Технологическая среда служит площадкой, с помощью которой совершаются киберпреступления. Согласно теории рационального выбора, преступление является результатом анализа человеком ожидаемых издержек и выгод, связанных с его преступной деятельностью. Например, в большинстве случаев спама и DDoS-атак киберпреступники часто осуществляют крупномасштабные скоординированные атаки, отправляя удаленные команды набору взломанных компьютеров (также известных как ботнеты). Высокопроизводительные компьютеры и соединения с высокой пропускной способностью, такие как университетские, корпоративные и государственные серверы, позволяют проводить более эффективные атаки и могут расширить сферу киберпреступности, что делает их предпочтительными для киберпреступников. Все этот может говорить о том, что технологический фактор положительно связан с киберпреступностью.

Готовность к кибербезопасности, включающая в себя юридические, технические, организационные аспекты, отражает возможности и приверженность страны к предотвращению и борьбе с киберпреступностью. Правовые меры, такие как законы и постановления, определяют, что представляет собой киберпреступность, и устанавливают необходимые процедуры расследования, судебного преследования и наказания за киберпреступления. Технические меры относятся к техническим возможностям, позволяющим справиться с рисками кибербезопасности и повысить защиту с помощью национальных учреждений и структур, таких как группы реагирования на различные инциденты или чрезвычайные ситуации в виртуальном пространстве [Евдокимов, 2021, с. 105].

Организационные меры относятся к комплексным стратегиям, политике, организациям и механизмам координации развития кибербезопасности. Развитие потенциала отражает исследования и разработки, информационные кампании, обучение и образование, а также рост сертифицированных специалистов и государственных учреждений для наращивания потенциала в области кибербезопасности. Меры сотрудничества подразумевают сотрудничество и обмен информацией на национальном, региональном и международном уровнях, что имеет важное значение для решения проблем кибербезопасности, учитывая транснациональный характер преступлений.

Среди исследователей киберпреступности общепризнано, что отсутствие стандартизированных юридических определений киберпреступности и достоверной и надежной официальной статистики затрудняет оценку распространенности или масштабов киберпреступности во всем мире. Хотя в некоторых странах правоохранительные органы собирают сведения о киберпреступлениях (например, данные полиции и судебные решения), неизбежны проблемы с занижением отчетности и недостаточной регистрацией этих официальных данных. Это побудило некоторых исследователей использовать альтернативные источники данных для измерения киберпреступности, включая социальные сети, онлайн-форумы, электронную почту и компании, занимающиеся кибербезопасностью. Среди этих источников можно выделить следующие: спам-сообщения или журналы брандмауэра, вредоносные домены/URL-адреса и IP-адреса, часто используемые для различных видов киберпреступности.

Однако из-за анонимности и виртуальности киберпространства преступники не ограничены национальными границами и могут использовать взломанные компьютеры, разбросанные по всему миру, в качестве платформы для совершения киберпреступлений. Между тем, IP-адреса могут быть подделаны с помощью таких технологий, как прокси-серверы, анонимные сети и виртуальные частные сети (VPN), с целью скрыть реальную личность и местонахождение киберпреступников [Рахманова, Пономарева, 2023, с. 203].

В результате, установление личности киберпреступника становится чрезвычайно сложной задачей и требует высокого уровня знаний и координации со стороны правоохранительных органов и групп кибербезопасности. Таким образом, вместо того, чтобы фиксировать местонахождение киберпреступников в физическом пространстве, большинство исследований с использованием этих технических данных вычисляют возможные места, где происходят кибератаки или киберпреступления, даже если часть из них могут быть местами, где киберпреступники предпочитают размещать свои бот-сети или спам-серверы [Поляков, 2020, с. 22].

Очевидно, что кибербезопасность играет ключевую роль в обеспечении безопасности не только глобальных предприятий и их инфраструктуры, но также безопасности и благополучия людей во всем мире, а также обеспечения процветания глобальной экономики.

Глобальная трансформация – это крупнейший поток перемен в современную эпоху, которого невозможно избежать. Изменения, вызванные глобализацией, имеют как положительные, так и отрицательные последствия. Глобализация усложнила национальным правительствам возможность принимать решения самостоятельно, изменив тем самым природу преступности [Сердечный, Скогорева, Длинный, 2021, с. 480]. Таким образом, тенденцией экономической преступности в глобальную эпоху являются преступления, основанные на высоких технологиях [Деникаева, Первышов, Гавришева, 2022, с. 28]. Вспышка экономических преступлений, связанных с высокими технологиями, порождает множество проблем, и их становится все труднее преодолеть [Жалыбина, 2021, с. 83].

Как и в случае с преступностью в целом, которая представляет собой сложную социальную проблему, она формируется из различных комплексных факторов, поэтому ее эффективное решение с помощью лишь частичного подхода невозможно. В связи с этим необходим макроподход в борьбе с экономическими преступлениями, связанными с технологиями. В этом случае макроподход трактуется как многоаспектный подход, занимающийся макроэкономическими проблемами [Жалыбина, 2021, с. 83].

Исходя из вышеизложенного, фундаментальные проблемы в правовом поле, особенно в сфере предпринимательской деятельности, в целях борьбы с преступностью в сфере электронных транзакций требует применения нормативно-правовых и концептуальных подходов, направленных на изучение применения новых правил или норм [Иванов, 2009, с. 85]. Законодательный подход абсолютно необходим для дальнейшего изучения применения закона о нарушениях/преступлениях в сфере электронных транзакций.

Заключение

Таким образом, возможные меры на макроуровне для эффективной кибербезопасности во всем мире включают повсеместное обучение граждан кибербезопасности, а также согласованная деятельность на уровне правительства по управлению рисками и информационными технологиями. Также важно регулировать соблюдение требований частными и государственными предприятиями.

Нельзя не упомянуть и о добровольном и всеобщем соблюдении всеми странами приемлемых кибернорм и международного права для ответственного поведения государства в киберпространстве. Страны должны сотрудничать друг с другом, с целью создания безопасного киберпространства и в вопросах об экстрадиции преступников, находящихся за рубежом. Предприятия, в свою очередь, должны создавать и поддерживать квалифицированные человеческие ресурсы в области кибербезопасности.

Наконец, все страны должны поощрять свободу Интернета и использовать модель управления с участием многих заинтересованных сторон, а также продвигать совместимую и надежную коммуникационную инфраструктуру и подключение к Интернету. Это приведет к созданию устойчивой экономики информации и знаний, что, в свою очередь, приведет к процветанию глобальной экономики в целом.

Библиография

1. Аникьева Э.Н., Дегтерева А.А. Интернет и киберпреступность // Наука и Образование. 2020. Т. 3. № 2. – С. 14.
2. Деникаева Р.Н., Первышов Е.А., Гавришева Е.В. Киберпреступность в финансовой (банковской) сфере // Экономика и управление: проблемы, решения. 2022. Т. 4. № 9 (129). – С. 26-32.
3. Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. д-ра юрид. наук. – М., 2021. – 557 с.
4. Жалыбина Е.В. Государственный механизм сдерживания киберпреступности в современных условиях развития общества // Право и вызовы нового мирового порядка. XXI век: Сборник материалов по итогам конкурса научных работ 2020 г. / под редакцией В.В. Беденкова. – Барнаул: Алтайский государственный университет, 2021. – С. 83-86.
5. Иванов В.М. Киберпреступность в условиях глобализации // Сборник научных трудов по материалам международной научно-практической конференции. 2009. Т.12. № 3. – С. 85-87.
6. Коваленко В.И. Инновационные технологии в комплексе оперативно-розыскного противодействия торговле людьми //Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов / под ред. В. С. Овчинского. – М.: ИНФРА-М.; 2021. – С. 365-402.
7. Поляков И.В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. 2020. № 4. – С. 21-25.
8. Рахманова Е.Н., Пономарева Е.В. Киберпреступность, цифровая преступность и кибербезопасность: проблемы определения и взаимосвязи // Уголовное право: стратегия развития в XXI веке. 2023. № 3. – С. 202-209.
9. Рыжов В.Б. Рыжов В.Б. Информационная безопасность в государствах Европейского союза: к постановке проблемы // Представительная власть – XX1 век. 2018. № 4. – С. 8-12.
10. Сердечный А.Л., Скогорева Д.А., Длинный Е.П. Картографическое исследование blockchain-транзакций и смарт-контрактов киберпреступников, атакующих автоматизированные информационные системы, и оценка ущербов от реализации их атак // Информация и безопасность. 2021. Т. 24. № 4. – С. 471-500.
11. Сухаренко А.Н. Транснациональные аспекты российской организованной киберпреступности // Информационное право. 2009. № 3. – С. 28-31.

Impact of the growth of cyber crime on global economic security

Grigorii A. Maistrenko

PhD in Law,
Senior Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
e-mail: G.Maystrenko@yandex.ru

Abstract

The article is devoted to the current problem of the growth of cybercrimes and their impact on economic security throughout the world. The concepts of hacking and online fraud, which bring a huge share of the profits of organized crime in most developed countries, are studied. The research task can be defined as assessing the risks of increasing cybercriminal activity in various areas of modern society. This paper attempts to create a conceptual model that analyzes cybercrime in the context of its impact on global socio-economic indicators, using a set of social, economic, political and technological indicators of cybersecurity as the main analytical tools. The authors come to the conclusion that cybercrime has a detrimental effect on the life, economy and international reputation of countries, and in this regard, the fight against cybercrime requires an integrated approach.

For citation

Maistrenko G.A. (2023) Vliyanie rosta kiberprestupnosti na obshchemirovuyu ekonomicheskuyu bezopasnost' [Impact of the growth of cyber crime on global economic security]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 12 (10A), pp. 59-64. DOI: 10.34670/AR.2024.17.66.008

Keywords

Cybercrime, Internet, hacking, cybersecurity, online fraud, organized crime.

References

1. Anikyeva E.N., Degtereva A.A. Internet and cybercrime // Science and Education. 2020. T. 3. No. 2. – P. 14.
2. Denikaeva R.N., Pervyshov E.A., Gavrisheva E.V. Cybercrime in the financial (banking) sector // Economics and management: problems, solutions. 2022. T. 4. No. 9 (129). – P. 26-32.
3. Evdokimov K.N. Combating computer crime: theory, legislation, practice: dis. Doctor of Law Sci. – M., 2021. – 557 p.
4. Zhalybina E.V. State mechanism for curbing cybercrime in modern conditions of social development // Law and challenges of the new world order. XXI century: Collection of materials based on the results of the competition of scientific works 2020 / edited by V.V. Bedenkova. – Barnaul: Altai State University, 2021. – pp. 83-86.
5. Ivanov V.M. Cybercrime in the context of globalization // Collection of scientific papers based on materials from the international scientific and practical conference. 2009. T.12. No. 3. – pp. 85-87.
6. Kovalenko V.I. Innovative technologies in the complex of operational-investigative counteraction to human trafficking // Operational-investigative activities in the digital world: collection of scientific works / ed. V. S. Ovchinsky. – M.: INFRA-M.; 2021. – pp. 365-402.
7. Polyakov I.V. Digital crime: problems of conceptual apparatus, systematization and law enforcement practice // Problems of law enforcement. 2020. No. 4. – pp. 21-25.
8. Rakhmanova E.N., Ponomareva E.V. Cybercrime, digital crime and cybersecurity: problems of definition and relationship // Criminal law: development strategy in the 21st century. 2023. No. 3. – P. 202-209.
9. Ryzhov V.B. Ryzhov V.B. Information security in the states of the European Union: towards the formulation of the problem // Representative power - XXI century. 2018. No. 4. – pp. 8-12.
10. Serdechny A.L., Skogoreva D.A., Dlinny E.P. Cartographic study of blockchain transactions and smart contracts of cybercriminals attacking automated information systems, and assessment of damage from the implementation of their attacks // Information and Security. 2021. T. 24. No. 4. – P. 471-500.
11. Sukharenko A.N. Transnational aspects of Russian organized cybercrime // Information law. 2009. No. 3. – P. 28-31.