Албегова Виктория Альбертовна
магистрант
Научный руководитель
Акоева Мадина Айларовна
канд. экон. наук, доцент

ФГБОУ ВО «Северо-Осетинский государственный
университет им. К.Л. Хетагурова»
г. Владикавказ, Республика Северная Осетия – Алания

DOI 10.31483/r-109298

ВЛИЯНИЕ КИБЕРУГРОЗ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ГОСУДАРСТВА

Аннотация*: противодействие современным вызовам и угрозам стало важнейшей задачей, влияющей на стратегические соображения поддержания стабильности в современном мировом порядке. Стремительное развитие информационной сферы сделало ее важнейшим компонентом общества. С ее дальнейшим развитием важность кибербезопасности становится еще более значимой. Кибербезопасность все теснее переплетается с различными аспектами национальной безопасности, включая политику, оборону и многое другое. В связи с этим изучение и решение проблем кибербезопасности являются важными для обеспечения устойчивого развития и защиты экономики государства.*

Ключевые слова*: экономическая безопасность, угроза, киберпреступность, государство, информационные технологии.*

С развитием информационных и коммуникационных технологий угрозы в сфере кибербезопасности становятся все более сложными и разнообразными.

Киберугрозы могут иметь серьезные последствия для экономики государства. Массовые хакерские атаки на компьютерные системы, сети и Интернет-инфраструктуру могут привести к потере конфиденциальных данных, финансо-

вых средств, нарушению бизнес-процессов и прекращению работы критически важных систем.

Государственные организации тоже могут стать мишенями кибератак, что может привести к политическим конфликтам и даже нарушению национальной безопасности.

В свете этих угроз кибербезопасность стала одним из приоритетных направлений для государственной политики, бизнес-сектора и общественности. Многие страны разрабатывают и внедряют меры по защите критической информационной инфраструктуры, укреплению законодательной базы и повышению осведомленности граждан и предприятий о кибербезопасности.

Растущая глобализация обмена информацией привела к тревожной тенденции переноса противоправной деятельности в виртуальную сферу. Киберпреступность, не знающая географических границ, представляет значительную угрозу национальным интересам и безопасности государств.

Поэтому странам необходимо уделять первостепенное внимание мерам кибербезопасности, чтобы обезопасить своих граждан и защитить национальные активы. Это включает в себя укрепление потенциала киберзащиты, развитие международного сотрудничества, повышение осведомленности населения об угрозах в Интернете, а также внедрение эффективных мер политики и регулирования. Эффективное решение проблем кибербезопасности позволит странам снизить потенциальные риски и обеспечить безопасность цифровой среды для своих граждан.

Тезаурус кибербезопасности охватывает различные элементы безопасности, включая информационную безопасность, безопасность приложений, сети, Интернета и критической информационной инфраструктуры. Как и традиционная информационная безопасность, кибербезопасность направлена на защиту активов с точки зрения трех составляющих безопасности: конфиденциальности, целостности и доступности. Однако кибербезопасность действует в контексте киберпространства, обеспечивая защиту в более абстрактных рамках.

Киберпреступность часто мотивируется различными целями, в том числе экономическими, политическими, идеологическими и социально-

психологическими. Экономические цели, как правило, связаны с получением финансовой выгоды за счет таких действий, как кража, мошенничество или вымогательство. Политические цели направлены на нанесение ущерба государственным институтам, нарушение властных отношений, подрыв доверия к власти. Идеологические цели могут заключаться в распространении экстремистской идеологии, вербовке людей в радикальные группировки, подстрекательстве к терроризму.

Наконец, социально-психологические цели направлены на нанесение морально-психологического ущерба людям, что может включать в себя такие действия, как распространение страха, унижение или преследование в Интернете. Важно отметить, что эти цели не являются взаимоисключающими, и киберпреступники могут руководствоваться несколькими мотивами своих действий.

Киберпреступность характеризуется следующими признаками: она совершается в виртуальном пространстве или компьютерных сетях.

Под виртуальным пространством понимается информационная сфера, создаваемая и моделируемая с помощью компьютеров, в которой хранятся данные о лицах, явлениях, фактах и процессах, представленные в символическом, математическом и других форматах. Эта информация передается по локальным и глобальным компьютерным сетям, находится в памяти различных виртуальных или физических устройств, специально предназначенных для хранения, передачи и обработки таких данных.

Усиление мер кибербезопасности играет важнейшую роль в снижении рисков и последствий киберпреступлений.

Основная задача кибербезопасности – оптимизировать управление программами кибербезопасности, сделав их доступными для принятия и реализации в своей среде предприятиями любого размера. Эти программы соответствуют уникальным требованиям, допустимым рискам и преобладающим угрозам, с которыми сталкивается каждая компания.

Следует отметить, что особенно подвержены кибератакам люди, использующие компьютеры как в личной, так и в профессиональной жизни, но обла-

дающие ограниченными знаниями основ кибербезопасности. Эта группа также подвержена воздействию вредоносных электронных устройств, направленных на компрометацию компьютерных систем, манипулирование компьютерными данными и использование уязвимостей в компьютерных сетях.

Обнаружение, предупреждение и борьба с киберпреступностью представляют собой сложную задачу, поскольку преступники часто используют различные обманные приемы для маскировки своей противоправной деятельности. В основе такой тактики часто лежат различные мотивы, такие как отказы носителей информации, неисправности электронных устройств или недостатки в конкретных программах, известные как «баги».

Для выявления киберпреступлений и задержания лиц, причастных к противоправной деятельности в сфере информационных технологий, было создано Управление «К». Это специализированное подразделение занимается расследованием и борьбой с преступлениями в сфере информационных технологий.

Таким образом, современная киберпреступность является не только следствием стремительного развития информационных технологий, но и значительной и высокодоходной сферой преступного поведения. Практически ни одна страна не остается незатронутой этой проблемой. Стремясь снизить риски в пределах своих границ, государства активно сотрудничают, оказывают взаимную поддержку и координируют усилия по борьбе с киберпреступностью.

Список литературы

1. Дементьева М.А. Киберпреступления в банковской сфере РФ: способы выявления и противодействия / М.А. Дементьева [и др.] // Экономические отношения. – 2021. – №2. – С. 109–120.

2. Добрынин Ю.В. Классификация преступлений, совершаемых в сфере компьютерной информации / Ю.В. Добрынин [Электронный ресурс]. – Режим доступа: http://www.russianlaw.net/law/computer_crime/al58/ (дата обращения: 11.12.2023).

3. Постановление Пленума Верховного Суда РФ «О судебной практике по уголовным делам о преступлениях экстремистской направленности» от 28 июня 2011 г. №11.

4. Чайковский Н.С. Статистика киберпреступности в Российской Федерации / Н.С. Чайковский, М.А. Кухенная // Оценка социально-экономического развития: опыт и перспективы: сб. материалов междунар. конф. (Донецк, 04–05 апр. 2021 г.). – Донецк. – С. 399–401.