Секция «Обеспечение экономической безопасности государства в условиях современных глобальных вызовов: экономико-правовые аспекты (совместно с Экономическим факультетом Белорусского государственного университета)»

Особенности обеспечения кибербезопасности в современных условиях

Научный руководитель – Гораева Татьяна Юрьевна

Бочарова Анна Александровна

Студент (бакалавр)

Белорусский государственный университет, Экономический факультет, Минск, Беларусь

E-mail: annabocharova2005@gmail.com

Потребность в безопасности для человека является одной из основных социальных нужд, которая сформировалась в социуме на грани инстинктивного и сознательного. С развитием общества категория «безопасность» стала охватывать интересы не только отдельного индивида, но и группы лиц, государства. В современных условиях в системе национальной безопасности стран мира выделяют военную, демографическую, социальную, экономическую и другие виды безопасностей, которые в совокупности обеспечивают стабильное функционирование государства.

Однако в связи со стремительной цифровизацией современного мира особую актуальность принимает понятие кибербезопасности. Каждый день миллионы людей совершают определенные действия в виртуальной среде, что создает условия для осуществления киберпреступлений. Киберугрозы оказывают воздействие на экономику страны, нанося вред как отдельным организациям, так и государству в целом. Эффективная политика в области кибербезопасности должна быть направлена не только на предотвращение кибермошенничества, но на создание безопасной цифровой среды, необходимой для устойчивого развития государства.

Под кибербезопасностью следует понимать совокупность методов, практик и технологий, обеспечивающих защиту компьютерных систем и сетей от цифровых атак. Термин «кибербезопасность» зародился в середине 1990-х гг. в США.

История данной сферы берет начало в 1972 году с создания первой антивирусной программы «Reaper» для удаления вируса «Creeper», разработанного для компьютерной сети ARPANET, предшественницы современного Интернета. С течением времени наблюдалась эволюция киберугроз, примером которых являются червь Морриса, один из самых первых масштабных вирусов, вирус Melissa, червь ILOVEYOU и другие попытки взлома различных организаций. В частности, ущерб от червя ILOVEYOU составил рекордные $15 миллиардов, что свидетельствует о серьезных потерях для мировой экономики и отдельных организаций. [3]

Вирусы и компьютерные черви являются формой проявления киберпреступности. При этом следует отметить, что киберпреступление — это вид преступления, совершаемого в интернете с использованием цифровых технологий. К основным видам можно отнести фишинг, кибер-сталкинг, вирусы, вредоносные атаки и онлайн-мошенничество.

С каждым годом по всему миру растет количество преступлений в интернет-пространстве. По статистическим данным в 2021 году в Республике Беларусь было зафиксировано около 13,4 тыс. киберпреступлений, в 2022 – приблизительно 11,7 тыс., в 2023 – 15,7 тыс. случаев, тогда как в 2024 году показатель увеличился на 8,3% и составил четверть от общего числа правонарушений в стране. В Российской Федерации также наблюдается тенденция роста данной ситуации: по данным Министерства внутренних дел РФ число киберпреступлений за 2021 год составило около 518 тыс., за 2022 год - около 510 тыс., за

2023 год возросло на 32%. В то же время за 2024 год было зарегистрировано 765,4 тыс. киберпреступлений, что эквивалентно 40% от общего числа преступлений. [5,6]

Для противостояния растущим киберугрозам, страны разрабатывают программы кибербезопасности и принимают законы, направленные на защиту от цифровых угроз. Например, 14 февраля 2023 года Президент Республики Беларусь подписал Указ № 40 "О кибербезопасности". Документом определяется правовая основа создания и функционирования национальной системы обеспечения кибербезопасности, предусматривающей формирование комплексного многоуровневого механизма противодействия кибератакам на государственные органы и организации. Конкретизированы задачи по обеспечению кибербезопасности государственных органов и иных организаций, закреплена персональная ответственность их руководителей, а также определены владельцы критически важных объектов информатизации. [4]

Что касается глобальных решений в сфере кибербезопасности, то в 2022 году в Европейском Союзе была принята Директива 2022/2555 (NIS2). Она требует от членов ЕС принять национальную стратегию и установить единую правовую базу для обеспечения кибербезопасности в важнейших отраслях по всему ЕС. Она также создает Европейскую сеть организации связи в случае кибератак и сеть групп реагирования на инциденты в сфере компьютерной безопасности. Данные нововведения позволят обеспечить обмен информацией между государствами о киберугрозах. [2]

Помимо методов борьбы с киберугрозами на законодательном уровне, также применяются различные технические и организационные методы, включая шифрование – метод перевода информации в набор символов, который невозможно расшифровать без ключа. Также важным элементом защиты является использование сетевых брандмауэров – защитных экранов, предназначенных для отслеживания и контроля потоков трафика в сети. Использование антивирусов и внедрение многофакторной аутентификации, регулярные аудиты безопасности и резервное копирование данных представляют собой необходимые методы борьбы с киберугрозами. [1]

Кибербезопасность представляет собой относительно новую сферу безопасности, стабилизирующую функционирование государства в современных условиях нарастания глобальных и локальных киберугроз. Ещё до недавнего времени не существовало единых правил для предотвращения киберпреступлений, но по мере роста их числа государства начали активно разрабатывать нормативные акты как на национальном уровне, так и на международном. Своевременное обеспечение безопасности цифровых систем позволяет предотвратить утечку данных, минимизировать финансовые потери. Кибербезопасность становится неотъемлемой частью поддержания экономической безопасности государства, так как гарантирует экономический рост в условиях цифровизации, защищает финансовые потоки, и поддерживает функционирование экономической системы.

Источники и литература

1) Борьба с киберугрозами: современные методы защиты данных и информационной безопасности: https://ifellow.ru/media-center/borba-s-kiberugrozami-sovremennye-metody-zashchity-dannykh-i-informatsionnoy-bezopasnosti/
2) Директива NIS2: новые правила кибербезопасности сетей и информационных систем: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
3) Кибербезопасность: https://iot.ru/wiki/kiberbezopasnost
4) О кибербезопасности: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g

5) Основные направления государственной политики в области информационной безопасности: https://minsk.gov.by/ru/actual/view/209/2022/inf_material_2022_12.shtml
6) Число киберпреступлений в России: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России