НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ РЕАЛИЗАЦИИ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВАХ ЕВРОПЕЙСКОГО СОЮЗА

REGULATORY AND LEGAL REGULATION OF THE IMPLEMENTATION OF THE STRATEGY OF CYBERSECURITY IN THE EUROPEAN UNION STATES

УДК 343. 9

Ковалев Олег Геннадьевич, доктор юридических наук, кандидат психологических наук, профессор, профессор кафедры организации режима и оперативно-розыскной деятельности в уголовно-исполнительной системе Псковского филиала Академии ФСИН России г. Псков.

Скипидаров Артём Алексеевич, магистрант ФГБОУ ВО Псковского государственного университета, г. Псков.

Kovalev O. G., okovalev66@gmail.com

Skipidarov A. A., temapskov@yandex.ru

Аннотация

В статье анализируется нормативно-правовое регулирование обеспечения кибербезопасности, структура и организационное построение органов ее обеспечивающих в государствах Европейского Союза. Рассматриваются законодательное закрепление понятийного аппарата, подходы в противодействии киберпреступности. Опыт и особенности реагирования на киберугрозы, кибератаки и киберинциденты, повышение киберустойчивости и киберкультуры на государственном, общественном и личностном уровнях. Делается исследовательский акцент на описании важных элементов, составляющих современную европейскую кибербезопасность

(кадровых, финансовых, исследовательских, образовательных, организационных, гендерных и других). Анализируются важнейшие документы в этой области, регламентирующие реализацию и планирование современной обновленной стратегии кибербезопасности в Евросоюзе с учетом трех базовых инициатив: нормативных, инвестиционных и политических, направленных на совершенствование киберустойчивости, технологического суверенитета и лидерства, взаимодействия и сотрудничества для развития глобального и открытого киберпространства.

Annotation

The article analyzes the regulatory and legal regulation of cybersecurity, the structure and organizational structure of the bodies providing it in the states of the European Union. The article considers the legislative consolidation of the conceptual apparatus, approaches to countering cybercrime. Experience and features of responding to cyber threats, cyber attacks and cyber incidents, improving cyber resilience and cyberculture at the state, public and personal levels. The research focuses on the description of the important elements that make up modern European cybersecurity (personnel, financial, research, educational, organizational, gender, and others). The article analyzes the most important documents in this area that regulate the implementation and planning of a modern updated cybersecurity strategy in the European Union, taking into account three basic initiatives: regulatory, investment and political, aimed at improving cyber resilience, technological sovereignty and leadership, interaction and cooperation for the development of a global and open cyberspace.

Ключевые слова: нормативно-правовое, киберпреступность, кибербезопасность, киберустойчивость, кибератаки, кибертерроризм, киберинциденты, киберкультура, кадровые, финансовые, исследовательские,

образовательные, организационные, гендерные, инвестиционные, политические.

Keywords: regulatory, cybercrime, cybersecurity, cyber resilience, cyberattacks, cyberterrorism, cyber incidents, cyberculture, personnel, financial, research, educational, organizational, gender, investment, political.

Государства Европейского Союза уделяют значительное внимание нормативно-правовому, организационному, методическому, материально-техническому, финансовому и кадровому обеспечению кибербезопасности как на союзном, так и внутригосударственном уровнях. При этом первостепенное значение придается осуществлению защиты персональных данных и информационной деятельности организаций, компаний и корпораций в киберпростаранстве, поддержанию работы онлайн-сообществ и экономики.

Еще в 2013 году в Европолиции был организован Европейский центр киберпреступности в целях усиления своевременного реагирования правоохранительных органов Евросоюза на современные вызовы, киберурозы, одной из которых является киберпреступность. За годы своего существования Центр внес значительный вклад в борьбу с киберпреступностью. Его сотрудники участвовали во многих резонансных специальных операциях, осуществляли организационную, оперативную и техническую поддержку в различных государствах. Результатом явились аресты сотен киберпреступников, проанализированы сотни тысяч файлов, подавляющее большинство из которых оказались вредоносными [1].

Чиновники Евросоюза убеждены, что киберпреступность является одним из приоритетов политического цикла организации, цели которого состоят в:

- пресечении криминальной деятельности, связанной с кибератаками на информационные системы так называемой бизнес-модели «преступление как услуга»;

- борьбе с сексуальным насилием над детьми и их сексуальной эксплуатацией, включая изготовление и распространение материалов о жестоком обращении с ними;

- преследование преступников, участвующих в мошенничестве и подделке безналичных платежных средств, включая крупномасштабное мошенничество с платежными картами.

Накопленный в странах Евросоюза богатый опыт правового регулирования и организации обеспечения безопасности, несомненно может быть полезен не только для отечественных ученых, специализирующихся на изучении рассматриваемой темы, но и для практических работников.

В связи с чем, нами было проведено теоретическое исследование правовых и некоторых организационных аспектов регламентации и интерпретации специальных подходов, терминологии и содержания кибербезопасности, противодействия киберугрозам и киберинцидентам в государствах Европейского Союза. В ходе исследования использовались методы сравнительного анализа, контент-анализа нормативных правовых документов Евросоюза по проблеме, а также документов, регламентирующие деятельность государственных и частных структур, общественных институтов и сообществ в вопросах противодействия киберугрозам и киберинцидентам, обеспечении кибербезопасности.

Важнейшей задачей для еврочиновников в настоящее время выступает реализация так называемой киберустойчивости, под которой понимается способность организаций и компаний обеспечивать высокую функциональность критически важных объектов инфраструктуры, непрерывно развивать государственные институты и бизнес [2].

Одним из первых современных правовых актов, регламентирующих деятельность европейских стран по поддержанию и повышению уровня кибербезопасности и киберустойчивости является Директива о безопасности

сетевых и информационных систем, принятая Европейским парламентом 6 июля 2016 года.

Данный нормативно-правовой документ определяет стратегию развития кибербезопасности, обязывает страны-члены Евросоюза принимать исчерпывающие меры по информационно-техническому оснащению национальных органов кибербезопасности, их своевременному реагированию на киберугрозы и киберинциденты.

Для координации совместных усилий, поддержания и облегчения стратегического сотрудничества в этом направлении, Директивой была создана специальная группа сотрудничества государств по обеспечению кибербезопасности, наделенная полномочиями операционного сотрудничества и обмена информацией о рисках киберугроз и киберинцидентов.

Другой заметной правовой новеллой рассматриваемого документа явилось закрепление в нем понятия культуры кибербезопасности, алгоритмизации своеобразного подсознательного реагирования заинтересованных должностных лиц на киберугрозы и киберинциденты в жизненно важных для экономики и общества сферах (энергетики, транспорта, водоснабжения, банковской системы, финансовых рынков, здравоохранения, цифровой инфраструктуры).

Этот культурный алгоритм обязывает компетентные государственные и коммерческие учреждения, ключевых поставщиков цифровых услуг (поисковые системы, службы облачных вычислений и онлайн-магазины) принимать необходимые меры безопасности, информировать о значительных киберинцидентах национальные правительства [3].

После принятия Директивы о безопасности сетевых и информационных систем, в том же году была создана Европейская организация по кибербезопасности для содействия Еврокомиссии в рамках договорного

государственно-частного партнерства на период до 2020 года. В ее состав вошли более 250 участников (представители промышленной индустрии кибербезопасности, исследовательские и образовательные организации в этой области, а также чиновники государственных структур и отраслей экономики, ориентированных на использование IT технологий и программного обеспечения. Кроме того, члены Европейской организации по кибербезопасности создают специальные общественные сообщества, оказывающие влияние на развитие промышленного производства в данной сфере в масштабах Евросоюза.

Центральным рабочим органом по вопросам кибербезопасности стало специально образованное Агентство Европейского Союза по сетевой и информационной безопасности, координирующее деятельность национальных структур в этой сфере, оказывающее методическую, организационную и практическую помощь государствам-членам ЕС, учреждениям и организациям, компаниям и предприятиям в практической реализации описанной выше Директивы.

Закон о кибербезопасности в Европейском Союзе, принятый в 2019 году, еще больше укрепил роль и значение Агентства, предоставив ему постоянный мандат на проведение необходимых информационно-аналитических и практических мероприятий и действий по предупреждению, выявлению, оперативному реагированию и разрешению киберинцидентов и киберугроз, а также управлению кризисами в Евросоюзе. Закон также наделил указанную структуру дополнительными финансовыми ресурсами, возможностями использовать квалифицированный персонал.

Рассмотренная Директива о безопасности сетевых и информационных систем была пересмотрена, дополнена и изменена в декабре 2020 года в сторону большей адаптации к современным потребностям и перспективам. В частности, был расширен список жизненно важных секторов, критичных для

экономики и общественных институтов, являющиеся мишенью киберугроз и киберинцидентов.

Также было введено понятие размера объектов этих секторов и их инфраструктуры, который автоматически распространил действие Директивы не только на крупные компании, корпорации, организации и предприятия, но и на средние. Одновременно государствам была предоставлена большая самостоятельность в регулировании средних и мелких предприятий и организаций с большим уровнем риска их кибербезопасности.

Кроме того, в новой Директиве устранено различие между операторами основных информационных услуг и поставщиками цифровых услуг, что повлекло за собой дифференциацию видов и степеней надзора за ними при обеспечении кибербезопасности.

Важным положением, направленным на унификацию законодательных правил в сфере кибербезопасности, нашедшим отражение в анализируемом документе, явилось определение минимального перечня базовых элементов безопасности для всех пользователей киберсетевого пространства. Установление единой процедуры и правил информирования о киберинцидентах, их содержании, сроков предоставления соответствующих отчетов, а также дальнейшую унификацию и гармонизацию режимов санкций в государствах Евросоюза.

В документе усиливается влияние Группы сотрудничества при подготовке единых стратегических политических решений в сфере новейших цифровых и IT технологий и тенденций, расширению обмена информацией и оперативного взаимодействия между властями государств, в том числе по предотвращению и преодолению киберкризисов. Также определяются ответственные участники управляемых и координируемых мероприятий по противодействию киберугрозам для Евросоюза, подготовки вместе с Агенством по кибербезопасности специального реестра в этой области [4].

Современные реалии также вносят свои коррективы в нормативно-правовое регулирование обеспечения кибербезопасности, нашедшие свое отражение в изучаемом документе, где она рассматривается как один из приоритетов в противодействии пандемии COVID-19, вызвавшей значительный рост кибератак в период введения режимов чрезвычайного реагирования, локдаунов и блокировок. Проведенный анализ плана восстановления Евросоюза в постпандемийный период показал выделение дополнительного финансирования на мероприятия, связанные с кибербезопасностью.

В Европейском Союзе большое внимание уделяется также финансированию специальных научных исследований и инноваций, призванных защитить государства и граждан от новейших модификаций киберугроз, реализуемых в виде конкретных киберинцидентов. В этих целях была принята и реализована так называемая программа Horizon 2020 в рамках которой осуществлялась финансовая, методическая, образовательная и технологическая поддержка субъектов кибербезопасности на протяжении семи лет. В частности, финансировались группы реагирования на инциденты, операторы и поставщики цифровых услуг, единые контактные центры, а также национальные органы, обеспечивающие кибербезопасность.

В настоящее время подобная программа Horizon Europe (на период 2021-2027годы), включенная в кластер «Гражданская безопасность для общества» с объемом инвестиций в систему кибербезопасности Евросоюза в размере 1,9 млд. евро находится в стадии обсуждения.

Параллельно существует и развивается фонд стратегических инвестиций, сочетающий государственное и частное финансирование обеспечения кибербезопасности.

Власти Европейского Союза уделяют значительное внимание координации деятельности в различных направлениях кибербезопасности. Для изучения, анализа и оценки опыта противодействия киберугрозам,

разрешения киберинцидентов разработана специализированная комплексная платформа Атлас кибербезопасности, которая также будет содержать вопросы классификации и стимулирования сотрудничества между экспертами в указанной сфере.

Кроме того, Комиссия Евросоюза предлагает создать новый Европейский центр компетенции в области промышленной и технологической кибербезопасности, который совместно с академическим сообществом и другими участниками будет определять приоритеты исследований и их практическое внедрение. В настоящее время свыше 170 партнерских организаций осуществляют четыре пилотных проекта по созданию данного центра.

Руководящими органами Европейского Союза подготовлен специальный план быстрого реагирования на чрезвычайные ситуации при крупномасштабном, трансграничном киберинциденте или кризисе. В нем изложены цели и способы сотрудничества государств с институтами ЕС в подобной ситуации. Для увеличения возможностей оперативного реагирования также планируется создание совместного кибер-подразделения в масштабах всего Союза.

В целях безопасного развертывания сетей 5G на территории Евросоюза предусматриваются меры по усилению требований к их безопасности, обеспечении диверсификации поставщиков, поскольку несмотря на огромные преимущества, эти технологии несут в себе дополнительные риски кибербезопасности (наличие большего числа потенциальных точек входа для злоумышленников из-за их менее централизованной архитектуры, количества антенн и повышенной зависимости от программного обеспечения).

Процесс цифровизации затронул и Европейские демократии, поэтому еврочиновники озабочены кибербезопасностью электронных выборов. Впервые такая проверка киберсистем на киберустойчивость была проведена непосредственно перед выборами в Европарламент в 2019 году.

Одним из приоритетных направлений стратегии кибербезопасности является кадровая составляющая, которой уделяется необходимое внимание. Проводятся мероприятия по поиску, рекрутированию и подготовке новых специалистов в области кибербезопасности в университетах, специальных центрах профессиональной подготовки. Финансирование и развитие так называемых обучающих «кибер-диапазонов», функционирующих в режиме моделирования киберугроз и инцидентов в режиме реального времени.

На наш взгляд, одним из важных, новаторских элементов стратегии кибербезопасности стран ЕС является учет человеческого фактора. Поскольку простое нажатие пользователем на фишинговую ссылку может привести к большим, часто непоправимым негативным последствиям. Поэтому уделяется внимание пользователей киберсетей, организаций, компаний и предприятий повышению осведомленности и компетентности. Ежегодно проводится Европейский месяц кибербезопасности.

Функционирующий объединенный исследовательский центр также является важным инструментом обеспечения кибербезопасности. Его сотрудники разработали таксономию кибербезопасности. Проанализировали исторические, организационные, правовые, технологические и технические аспекты, современное состояние и тенденции развития, представив результаты исследования в специальном отчете под названием «Кибербезопасность – наш цифровой якорь».

Руководители Еврокомиссии уделяют внимание и гендерной политике в обеспечении кибербезопасности. С использованием средств массовой информации осуществляется поиск и рекрутирование талантливых женщин, которые становятся все более узнаваемыми в киберсообществе и в общественных дебатах, принимают участие в конкретных мероприятиях по реагированию на киберугрозы и инциденты, обеспечивая таким образом высокий уровень кибербезопасности.

Таким образом, принятая в декабре прошлого года стратегия кибербезопасности Европейского Союза направлена на обеспечение глобального и открытого Интернета с надежными гарантиями там, где есть риски для безопасности и нарушения прав и законных интересов жителей Европы.

Развивая принципы и достижения предыдущих стратегий, документ содержит конкретные предложения по использованию трех базовых инициатив: нормативных, инвестиционных и политических по трем основным направлениям совершенствования:

- киберустойчивости, технологического суверенитета и лидерства. Технологический суверенитет должен быть основан на устойчивости всех подключенных услуг и продуктов. Основные четыре киберсообщества, связанные с внутренним рынком, правоохранительными органами, дипломатией и обороной должны более тесно сотрудничать в целях общего понимания угроз, быть готовыми к коллективному реагированию в случае материализации киберугрозы в конкретную кибератаку или киберинцедент;

- оперативного потенциала предотвращения, сдерживания и реагирования на киберугрозы и киберинциденты;

- взаимодействие и сотрудничество для развития глобального и открытого киберпространства.

Положения стратегии определяют нормы для решений мирового уровня, формулируют стандарты кибербезопасности для основных услуг и критически важных инфраструктур. Стимулируют разработку и применение новых технологий. Правительства, предприятия и граждане разделят ответственность за обеспечение кибербезопасной цифровой трансформации.

Проведенный в процессе исследования анализ основных нормативных правовых документов Европейского Союза в рассматриваемой сфере показал, что союз намерен и в дальнейшем всемерно поддерживать и развивать

стратегию кибербезопасности путем беспрецедентного уровня инвестиций в переходный период к цифровым технологиям в течение следующих семи лет. Увеличение размера финансирования мероприятий по обеспечению кибербезопасности более чем в четыре раза в сравнении с предыдущим бюджетом выделенным на эти цели, наглядно демонстрирует приверженность ЕС современной, обновленной технологической и промышленной политике и программе восстановления, преодоления последствий пандемии.

Литература

1. Ссылка: www.europol.europa.eu [сайт]. - URL: http://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3(дата обращения 12.02.2021)
2. Ссылка: www.ec.europa.eu [сайт]. - URL: http://www.ec.europa./eu/digital-single-market/en/cybersecurity#Strategy (дата обращения 12.02.2021)
3. Ссылка: www.eur-lex.europa.eu [сайт]. - URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата обращения 10.02.2021)
4. Ссылка: www.ec.europa.eu [сайт]. - URL: http://www.ec.europa/ newsroom/dae/document.cfm?doc_id=72166 (дата обращения 11.02.2021)

Literature

1. Link: www.europol.europa.eu [website]. - URL: http://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3(accessed: 12.02.2021)
2. Link: www.ec.europa.eu [website]. - URL: http://www.ec.europa./eu/digital-single-market/en/cybersecurity#Strategy (accessed: 12.02.2021)

3. Link: www.eur-lex.europa.eu [website]. - URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (accessed: 10.02.2021)

4. Link: www.ec.europa.eu [website]. - URL: http://www.ec.europa/newsroom/dae/document.cfm?doc_id=72166 (accessed: 11.02.2021)