DOI 10.21672/1818-510X-2019-60-3-073-078

ПОЛИТИКА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ЕВРОПЕЙСКОМ СОЮЗЕ: НАЦИОНАЛЬНЫЙ И НАДНАЦИОНАЛЬНЫЙ УРОВНИ

Кардава Николай Вахтангович, младший научный сотрудник
Национальный исследовательский институт мировой экономики
и международных отношений им. Е. М. Примакова РАН
Российская Федерация, 117997, г. Москва, ГСП-7, ул. Профсоюзная, 23
E-mail: kardava98@mail.ru

Рассмотрены актуальные вопросы, связанные с проблемой обеспечения кибербезопасности Европейского союза на национальном и наднациональном уровнях регулирования киберпространства. Отмечено, что в связи с ростом угроз в киберпространстве изменяются функции национального государства в сфере кибербезопасности. Национальное государство передаёт часть своих функций наднациональным органам ЕС, которые определяют стратегию в этой области. Однако в результате делегирования части функций наднациональным органам в сфере кибербезопасности возникают противоречия, связанные с различным уровнем развития государств в ЕС, с различными культурными традициями, разной обеспеченностью кадрами. Фактически в ЕС проводится эксперимент по взаимодействию национальных и наднациональных органов, причём окончательные результаты этого эксперимента пока неясны. Приводится статистика киберпреступлений в Европейском союзе до и после 2014 г. Показывает, как киберпреступность, кибератаки, хакерство могут повлиять не только на безопасность в киберпространстве, но и на общественную и национальную безопасность государства в целом.

Ключевые слова: кибербезопасность, национальное регулирование, наднациональное регулирование, киберпреступность, кибератаки, киберпространство, киберугрозы, Европейский союз, Германия, Швеция, кибертерроризм, киберзащита

CYBERSECURITY POLICY IN THE EUROPEAN UNION: NATIONAL AND SUPRANATIONAL LEVELS

Kardava Nikolay V., Junior Researcher
Primakov National Research Institute of World Economy and International Relations, RAS
23 Profsoyuznaya St., GSP-7, Moscow, 117997, Russian Federation
E-mail: kardava98@mail.ru

This article is dedicated to topical issues connected with ensuring of cyber security in the European Union on national and supranational levels of cyberspace regulation. The article states that due to the growing threats in cyberspace the role of national government in cyber security sector is changing. The nation-state is delegating part of its responsibilities to the supranational bodies of the EU which in their turn determine the strategy in this sphere. However, this leads to various contradictions that are caused by different development level of the EU countries, different cultural traditions and different personnel availability. The EU is in fact conducting an experiment in cooperation between national and supranational bodies, and the results are not yet clear. The article also provides statistics of cybercrimes in the European Union before and after 2014. The author shows how cyber crime, cyber attacks and hacking can affect not only security in cyberspace itself, but also national security in general and the level of security society currently provides for its members.

Keywords: cybersecurity, national regulation, supranational regulation, cybercrime, cyberattacks, cyberspace, cyber threats, European Union, Germany, Sweden, cyberterrorism, cybersecurity

В современных условиях в силу чрезвычайно быстрого развития информационных технологий проблема обеспечения кибербезопасности является одной из важнейших задач для государственных органов, частного бизнеса, отдельных граждан и для общества в целом. *Кибербезопасность можно определить как совокупность профилактических и реактивных действий, направленных на защиту от угроз конфиденциальности пользователей в киберпространстве, на обеспечение целостности и доступности компьютеров, сетей и информации*, которые составляют *киберпространство – концептуальное пространство, обеспечивающее оцифрованную и сетевую деятельность граждан и организаций*.

Нами проведён анализ основных тенденций и противоречий политики обеспечения кибербезопасности в Европейском союзе (ЕС) на национальном и наднациональном уровнях. Актуальность этой проблемы связана с тем, что взаимодействие национальных государств в этой области является наиболее продвинутым и тесным именно в ЕС. В то же время на примере стран ЕС можно увидеть многочисленные проблемы и противоречия регулирования киберпространства, связанные с взаимодействием национальных государств и наднациональных образований. Таким образом, соотношение национального и наднационального уровней обеспечения кибербезопасности представляет собой не только технологическую, но прежде всего политическую проблему, которая имеет как региональное, так и глобальное значение. Кроме того, некоторые аспекты деятельности ЕС в области кибербезопасности могут представлять интерес для России и Евразийского экономического союза (ЕАЭС).

Обеспечение кибербезопасности на уровне национальных государств ЕС. В отношении противодействия киберугрозам страны ЕС можно разделить на две категории: группу стран со «средней эффективностью» и группу наиболее отсталых стран. Учитывая глобальный характер киберпространства и отсутствие в нём национальных границ, органы ЕС, как правило, пытаются проводить единую политику кибербезопасности для всех стран, издают директивы, создают регулирующие органы, разрабатывают стратегии. Однако при этом обнаруживаются противоречия между противодействием киберугрозам на национальном и наднациональном уровнях: не все страны ЕС могут полностью реализовать эти директивы и стратегии, в том числе и из-за различного технического, социального и экономического уровня развития.

Среди стран ЕС в области разработки и применения национальных стратегий кибербезопасности наиболее передовыми являются Австрия, Венгрия, Нидерланды, Норвегия, ФРГ, Швеция, Эстония. Наименее развиты в области кибербезопасности такие страны, как Бельгия, Болгария, Греция, Португалия, Румыния.

Имеет смысл остановиться на обеспечении кибербезопасности и информационной безопасности в ФРГ как наиболее экономически развитой стране ЕС, являющейся мотором европейской интеграции. Стратегия безопасности в киберпространстве в Германии была принята в начале 2011 г., при этом в Стратегии ФРГ основное внимание уделено предотвращению и уголовному преследованию кибератак, а также предупреждению выхода из строя IT-оборудования, которое может быть вызвано случайными факторами. Кроме того, в Стратегии Германии проводится анализ необходимости дополнительных действий по защите IT-систем посредством предоставления основных функций безопасности, сертифицированных государством, а также поддержки малого и среднего бизнеса путём создания специальной рабочей группы.

В дополнении к этому 11 июля 2015 г. парламентом ФРГ был принят закон о кибербезопасности, согласно которому более 2000 поставщиков услуг обязаны внедрить новые стандарты безопасности в киберпространстве в течение двух лет; в противном случае немецким компаниям грозит штраф на сумму 100 тыс. евро. Закон оказывает влияние на институты, перечисленные в качестве «критической инфраструктуры», включая такие системы, как транспорт, здравоохранение, водоснабжение, коммунальные услуги, провайдеры телекоммуникационных услуг, а также финансовые и страховые компании. При этом новый закон обязывает компании уведомлять о любых кибератаках в Федеральное управление по информационной безопасности Германии (BSI) [2].

Национальная стратегия Австрии в области безопасности информационно-коммуникационных технологий (ИКТ) использует более широкую концепцию безопасности ИКТ и рассматривает кибербезопасность и киберзащиту в качестве жизненно важных и комплексных, но преимущественно реактивных стратегий. Однако ни кибербезопасность, ни киберзащита не могут применяться эффективно, если они не дополняются элементами проактивной (предохраняющей) стратегии в более широком масштабе. Стратегия безопасности ИКТ является инициативной концепцией, направленной на защиту киберпространства и людей в этом виртуальном пространстве с учётом их основных прав и свобод. Конкретный подход страны к кибербезопасности тесно связан с существующими в ней наиболее заинтересованными сторонами и структурами – различными организациями, учреждениями или отдельными лицам.

Ещё одной страной ЕС, в которой развита система кибербезопасности, является Швеция. Относительно высокий уровень киберзащиты в Швеции объясняется экономической и социальной развитостью страны, а также дисциплинированностью её граждан и в целом благополучной криминогенной ситуацией. Но и в Швеции вопросы компьютерной безопасности не всегда оказываются на высоте. Пробелы возникают, как правило, там, где сталкиваются или пересекаются интересы различных ведомств или групп. Кроме того, в Швеции отсутствует централизация ответственности за кибербезопасность, нет центрального координирующего органа, отвечающего за обеспечение кибербезопасности в стране. Эта ответственность распределена между четырьмя министерствами и восьмью ведомствами, что препятствует разработке эффективных мер по быстрой и согласованной реакции на киберугрозы.

В целом можно констатировать, что политика обеспечения кибербезопасности на уровне отдельных национальных государств в ЕС не является достаточно эффективной, т. к. киберпространство имеет наднациональный, точнее глобальный характер. По этой причине ЕС проводит политику в области кибербезопасности на наднациональном, общеевропейском уровне.

Политика кибербезопасности в ЕС на наднациональном уровне. 23 ноября 2001 г. в Будапеште была подписана Конвенция Совета Европы «О киберпреступности». Это один из важнейших документов, регулирующих правоотношения в сфере глобальной информационной сети по предотвращению и контролю преступности, связанной с применением компьютеров [1, с. 152].

В Конвенции Совета имеются определения киберпреступлений, совершённые в информационном пространстве. Особое место уделяется вопросам взаимодействия стран на национальном и наднациональном уровнях, которые направлены на пресечение несанкционированного вмешательство в работу компьютерных систем.

Комплекс Директив ЕС по развитию информационного общества в сумме охватывают существенную часть спектра вопросов кибербезопасности. При этом директивы ЕС не преследуют конкретную цель обеспечения кибербезопасности, но выстраивают модель регулирования преимущественно на основе интересов внутреннего европейского рынка.

В 2004 г. в рамках ЕС было создано Европейское агентство по сетевой и информационной безопасности (ENISA), координирующее деятельность стран союза для борьбы с киберугрозами. В последнее время Евросоюз проявляет всё больше активности в вопросах обеспечения кибербезопасности в рамках данного агентства. Его задачей является обеспечение высокого уровня сетевой и информационной безопасности в странах Евросоюза. В 2006 г. Евросоюз принял Стратегию безопасного информационного общества.

Среди органов, которые на сегодняшний момент ведут борьбу с киберпреступностью на наднациональном уровне ЕС, можно выделить следующие институты:

- Европол (обучение национальных полицейских структур, судей и прокуроров, работающих в области борьбы с киберпреступностью);
- Евроюст (агентство Европейского союза, имеющее дело с судебными органами);
- Европейское агентство по сетевой и информационной безопасности (ENISA) [3, с. 1].

Интерпол по соглашению с Советом Европы является партнёром и руководит осуществлением правоохранительного компонента проекта. Другими партнёрами по проекту являются Эстония (Министерство юстиции), Франция (Министерство внутренних дел), Румыния (Национальная полиция, прокуратура (DIICOT) и Министерство юстиции), Соединённое Королевство (Национальное агентство по борьбе с преступностью) и США (Министерство юстиции), а также Европол (Европейский центр по киберпреступности).

Европейская комиссия пытается бороться с распространением в социальных сетях пропаганды терроризма, проявлений ксенофобии и «языка вражды» (hate speech), а также публикаций, нарушающих авторские права. Комиссия отметила увеличение готовности высокотехнологичных компаний сотрудничать с национальными и наднациональными правоохранительными органами по вопросам борьбы с противоправным контентом. В пресс-релизе Европейской комиссии за 2017 г. особо подчёркивалась социальная ответственность онлайн-платформ с точки зрения защиты пользователей и общества в целом от киберугроз [8]. В то же время ЕС достаточно поздно (в 2008 г.) пришёл к пониманию киберугроз как ключевого вызова безопасности, имеющего не только экономическое и политическое, но и военное измерение. До этого времени ЕС занимался в основном противодействием киберпреступности и кибертерроризму. Государства-члены ЕС прошли долгий и трудный путь к выработке общей внешней политики и политики безопасности, которая представляет собой сложную совокупность мер, требующую многочисленных согласований. По этой причине эта политика отвечает на происходящие изменения с большим промедлением, что сказывается на эффективности обеспечения кибербезопасности и общей безопасности в странах Евросоюза.

В декабре 2018 г. Европейский парламент, Совет Европейского союза и Европейская комиссия сформировали политическое соглашение по закону о кибербезопасности. С этого момента ENISA (первоначально «Агентство по сетевой и информационной безопасности») стало именоваться «Агентство ЕС по кибербезопасности».

Основные моменты закона о кибербезопасности состоят в следующем:

- ENISA получает постоянный мандат на деятельность в области обеспечения кибербезопасности, при этом обеспечивается значительными людскими и финансовыми ресурсами.
- ENISA увеличивает свою поддержку государствам-членам ЕС, чтобы улучшить их возможности и опыт, в частности, в области противодействия киберкризисам, предотвращения и реагирования на киберинциденты.
- В рамках сертификации кибербезопасности ENISA будет выполнять задачи, связанные с рынком киберуслуг, в частности, путём подготовки европейских норм и процедур

сертификации кибербезопасности при экспертной помощи и в тесном сотрудничестве с национальными сертификационными органами и промышленностью.

- ENISA усилит свою поддержку государствам-членам и институтам ЕС в разработке, реализации и обзоре общей политики кибербезопасности [9].

В 2016 г. в рамках проекта Европейской комиссии под названием «Горизонт 2020» на обеспечение кибербезопасности было выделено 450 млн евро. Общее количество инвестиций в этой области к 2020 г. планируется довести до 1,8 млрд евро.

Инициативы Европейской комиссии направлены в первую очередь на защиту от кибератак и увеличение конкурентоспособности сектора IT-безопасности. Еврокомиссия планирует запустить публичный проект партнерства под эгидой программы «Горизонт 2020» и привлечь дополнительные средства от участников Европейской организации по кибербезопасности (ECSO). Политики ожидают утроить размер инвестиций от частного сектора.

Взаимодействие политики обеспечения кибербезопасности на национальном и наднациональном уровнях. Итак, ЕС пытается последовательно проводить согласованную и единую политику обеспечения кибербезопасности на наднациональном уровне [6, p. 299–300]. В то же время в ЕС по-прежнему существуют национальные государства, каждое из которых имеет собственное законодательство, свою политическую систему, свой уровень экономического развития и другие особенности. Каждое из этих государств пытается по-своему регулировать киберпространство и обеспечивать кибербезопасность, т. е. проводить собственную политику в этой области. Отсюда возникает проблема взаимодействия национального и наднационального уровней политики обеспечения кибербезопасности в ЕС.

Проблема соотношения национальных и наднациональных стратегий в области кибербезопасности заключается в том, что страны ЕС сильно разобщены по уровню технологического и социально-экономического развития. На наднациональном уровне Европейский союз не оказывает напрямую техническую помощь государствам-членам, но призывает их к применению передовых практик. ЕС также сталкивается с проблемой дублирования функций в области кибербезопасности с такой влиятельной международной военно-политической организацией, как НАТО.

Далеко не все члены ЕС рассматривают кибербезопасность в качестве приоритета национальной безопасности. Отсутствие единого понимания угроз кибербезопасности в ЕС также снижает возможности по обеспечению безопасности его членов. Рассмотрение вопросов кибербезопасности до сих пор остается фрагментированным и часто происходит в пределах национальных границ. В 2017 г. в Финляндии создан Европейский центр по противодействию гибридным угрозам, сотрудничающий с ЕС и НАТО. Основной целью центра является исследовательская работа, однако перечень отчётов показывает, что речь идёт не просто о науке и аналитике, а о разработке потенциальных доктринальных принципов в области обеспечения кибербезопасности [4].

В ЕС учреждены общеевропейские агентства по организации сотрудничества правоохранительных органов, судебных органов, ведомств, регулирующих информационную и сетевую безопасность. Сотрудничество с национальными компетентными структурами осуществляется в постоянном режиме 24/7 (24 ч в сутки, 7 дней в неделю) [5, с. 721]. Одним из важных положительных особенностей европейского подхода в области кибербезопасности является последовательная и целенаправленная политика, направленная на нахождение баланса между национальной и наднациональной компетенциями. Общеевропейские структуры, как правило, не подменяют собой национальные ведомства, но являются координирующими центрами, предоставляют информационную, экспертную и техническую поддержку.

В то же время в связи с чрезвычайно быстрым развитием информационных технологий, а также с их внедрением во все сферы жизни общества и граждан политика ЕС, направленная на противодействие киберугрозам, сталкивается всё с новыми и новыми вызовами, требующими более быстрого и эффективного реагирования [7, p. 29].

Эффективность политики обеспечения кибербезопасности в ЕС и ущерб от кибератак. По данным, приведённым главой Европейской комиссии Жан-Клодом Юнкером в 2016 г., 86 % европейцев считали, что риск стать жертвой киберпреступников растёт. Такие сектора, как транспорт, энергетика, здравоохранение и финансы, становятся всё более зависимыми от сетей и информационных систем для ведения своего основного бизнеса.

В докладе Европейской комиссии говорится, что в 2016 г. 80 % европейских компаний сталкивались по крайней мере с одним случаем, связанным с нарушением кибербезопасности. В 2016 г. число атак со стороны вымогателей достигло 4000. Все эти явления и вызовы

отчасти связаны с тем, что европейцы доверяют цифровым технологиям, подчас чрезмерно. Эти технологии открывают перед гражданами новые возможности для установления связей, содействия распространению информации и формирования основы европейской экономики. Однако они также создают новые риски, поскольку негосударственные и государственные субъекты всё чаще пытаются украсть данные, совершить мошенничество или даже дестабилизировать в разных странах работу правительств и политическую ситуацию в целом [12].

Согласно опросу "Eurobarometer", проведённому в 2014 г., европейцы очень обеспокоены проблемами кибербезопасности. Около 68 % пользователей интернета в странах ЕС обеспокоены кражей личных данных и обнаружением вредоносного программного обеспечения на своих устройствах [13, p. 4]. Более половины опрошенных европейцев волнует перспектива стать жертвой кражи с банковских карт или интернет-банкинг мошенничества, взлом аккаунтов по электронной почте, подложные электронные письма или телефонные звонки, онлайн-мошенничества и случайные обнаружения детской порнографии в интернете [13, p. 4–5]. Кроме того, не будучи в состоянии получить доступ к онлайн-сервисам из-за кибератак и кибервымогательства, пользователи могут случайно столкнуться с материалом, который пропагандирует расовую ненависть и религиозный экстремизм.

По данным экспертов из Совета Европы, мошеннические действия, связанные с кредитными картами, уносят ежегодно около 400 млн долл., ущерб от вирусных атак составляет примерно 12 млрд долл, а нарушение прав интеллектуальной собственности наносит ущерб порядка 250 млрд долл. [1, с. 131].

В такой развитой стране, как Германия, где проводится относительно эффективная политика обеспечения кибербезопасности, киберпреступность продолжает расти, причём, по данным полиции, раскрывается только одно преступление из четырех, а полицейские союзы считают, что до 90 % интернет-преступлений остаются незарегистрированными [11]. В 2016 г. правительство Германии зарегистрировало 82649 случаев компьютерного мошенничества, шпионажа и других киберпреступлений, что на 80 % больше, чем в 2015 г. [10]. По данным немецкой полиции, в том же 2016 г. было зарегистрировано 253290 случаев преступлений, совершённых в интернете, что на 3,6 % больше по сравнению с 2015 г. При этом в ФРГ от кражи личных данных ежегодно страдают около 16 млн человек. Эти и другие данные свидетельствуют о том, что несмотря на проводимую в ЕС политику противодействия киберугрозам и обеспечения кибербезопасности на национальном и наднациональном уровнях, в целом эффективность этой политики остается не слишком высокой. Такая ситуация требует дальнейшей разработки в странах ЕС более согласованных мер по обеспечению кибербезопасности и более быстрого реагирования на возникающие новые киберугрозы. Сталкиваясь с постоянно растущими вызовами и угрозами кибербезопасности, ЕС вынужден непрерывно совершенствовать свою политику в области кибербезопасности для своевременного реагирования на кибератаки, направленные на государства-члены или на институты ЕС.

По итогам исследования можно сделать вывод, что с учётом взаимодействия национальных и наднациональных органов ЕС политика обеспечения кибербезопасности сталкивается с целым рядом проблем и трудностей. Несмотря на множество законодательных и других актов ЕС в области кибербезопасности, а также на создание различных национальных и наднациональных органов, система мер по обеспечению кибербезопасности недостаточно сформирована и недостаточно эффективна. Одна из основных причин заключается в том, что руководство ряда европейских государств лишь за последние годы приняло решение реализовать единую политику в области кибербезопасности. Помимо этого важным обстоятельством, мешающим проведению единой согласованной политики, является то, что члены ЕС существенно различаются по экономическим, техническим и военным возможностям. Поэтому одни страны ЕС (как, например, Германия, Норвегия или Швеция) более развиты в области кибербезопасности и киберзащиты, чем другие (например, Греция или Бельгия). Система защитных мер в области кибербезопасности на национальном и наднациональном уровнях интенсивно развивается, но при этом сталкивается с многочисленными трудностями в согласовании решений и выработке единой политики обеспечения кибербезопасности. Очевидно, что эта политика нуждается в дальнейшем совершенствовании. Тем не менее, опыт обеспечения кибербезопасности в странах ЕС может быть весьма полезен для Российской Федерации и для стран ЕАЭС в плане разработки нормативных актов и подходов к согласованию мер по обеспечению кибербезопасности на межрегиональном и межстрановом уровнях.

Список литературы

1. Господарик, Ю. П. Международная экономическая безопасность / Ю. П. Господарик, М. В. Пашковская. – Москва : Московский финансово-промышленный университет «Синергия», 2016. – 416 с.
2. Есмуханова, А. Кибербезопасность в международном и национальном законодательстве, 2016 г. / А. Есмуханова, А. Кази. – Режим доступа: https://zerde.gov.kz/activity/ict/publication/2221/, свободный. – Заглавие с экрана. – Яз. рус.
3. Марин, Н. Интернет-преступность и Европейский союз / Н. Марин, З. Гергинова. – Режим доступа: https://cybersafetyunit.com/internet-prestupnost-i-evropeyskiy-soyuz/, свободный. – Заглавие с экрана. – Яз. рус.
4. Скворцова, Е. Военизация дискурса кибербезопасности как угроза международной стабильности / Е. Скворцова. – Режим доступа: https://www.icisecurity.ru/publications/studenty_i_aspiranty/ekaterina-skvorcova-2018/, свободный. – Заглавие с экрана. – Яз. рус.
5. Шматкова, Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы / Л. П. Шматкова // Молодой ученый. – 2016. – № 28 (132). – Режим доступа: https://moluch.ru/archive/132/37021/, свободный. – Заглавие с экрана. – Яз. рус.
6. Carrapico, H. European Union cyber security as an emerging research and policy field / H. Carrapico, A. Barrinha // European Politics and Society. – 2018. – Vol. 19, № 3. – P. 299–303.
7. Christou, G. Cybersecurity in the European Union. Resilience and adaptability in governance policy / G. Christou. – London : Palgrave, 2016. – 222 p.
8. Communication from the Commission to the European Parliament, the council, the European economic and social committee and the committee of the regions. – Режим доступа: https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms, свободный. – Заглавие с экрана. – Яз. англ.
9. EU leaders agree on ground-breaking regulation for cybersecurity agency ENISA, 2018. – Режим доступа: https://www.enisa.europa.eu/news/enisa-news/eu-leaders-agree-on-ground-breaking-regulation-for-cybersecurity-agency-enisa, свободный. – Заглавие с экрана. – Яз. англ.
10. German cyber crime rose 80 percent in 2016: report. – Режим доступа: https://www.reuters.com/article/us-germany-crime-cyber/german-cyber-crime-rose-80-percent-in-2016-report-idUSKBN17P0YB, свободный. – Заглавие с экрана. – Яз. англ.
11. Police struggle as cybercrime hits record. – Режим доступа: https://www.thelocal.de/20140603/internet-crime-in-germany-at-a-record-high, свободный. – Заглавие с экрана. – Яз. англ.
12. Resilience, Deterrence and Defence: Building strong cybersecurity in Europe. – European Commission, State of the Union, 2017.
13. Special Eurobarometer 423. Cybersecurity. – European Union, 2015. – 160 p.

References

1. Gospodarik Yu. P., Pashkovskaya M. V. *Mezhdunarodnaya ekonomicheskaya bezopasnost* [International economic security]. Moscow, Moscow Financial and Industrial University “Sinergiya” Publ., 2016, 416 p.
2. Esmukhanova A., Kazi A. *Kiberbezopasnost v mezhdunarodnom i natsionalnom zakonodatelstve* [Cybersecurity in international and national law]. Available at: https://zerde.gov.kz/activity/ict/publication/2221/.
3. Marin N., Gerginova Z. Internet prestupnost i Evropeyskiy soyuz [Internet crime and the European Union]. Available at: https://cybersafetyunit.com/internet-prestupnost-i-evropeyskiy-soyuz/.
4. Skvortsova E. *Voenizatsiya diskursa kiberbezopasnosti kak ugroza mezhdunarodnoy stabilnosti* [Militarization of cybersecurity discourse as a threat to international stability]. Available at: https://www.icisecurity.ru/publications/studenty_i_aspiranty/ekaterina-skvorcova-2018/.
5. Shmatkova L. P. Mezhdunarodnoe sotrudnichestvo v borbe s kiberprestupleniyami: sostoyanie i perspektivy [International cooperation in the fight against cybercrime: status and prospects]. *Molodoy uchenyy* [Young scientist], 2016, no. 28 (132), p. 1.
6. Carrapico H., Barrinha A. European Union cyber security as an emerging research and policy field. *European Politics and Society*, 2018, vol. 19, no. 3, pp. 299–303.
7. Christou G. *Cybersecurity in the European Union. Resilience and adaptability in governance policy*. London, Palgrave Publ., 2016, 222 p.
8. Communication from the Commission to the European Parliament, the council, the European economic and social committee and the committee of the regions. Available at: https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms.
9. EU leaders agree on ground-breaking regulation for cybersecurity agency ENISA. Available at: https://www.enisa.europa.eu/news/enisa-news/eu-leaders-agree-on-ground-breaking-regulation-for-cybersecurity-agency-enisa.
10. *German cyber crime rose 80 percent in 2016: report*. Available at: https://www.reuters.com/article/us-germany-crime-cyber/german-cyber-crime-rose-80-percent-in-2016-report-idUSKBN17P0YB.
11. *Police struggle as cybercrime hits record*. Available at: https://www.thelocal.de/20140603/internet-crime-in-germany-at-a-record-high.
12. *Resilience, Deterrence and Defence: Building strong cybersecurity in Europe*. European Commission, State of the Union Publ., 2017.
13. *Special Eurobarometer 423. Cybersecurity*. European Union Publ., 2015. 160 p.