

DOI 10.32726/2411-3417-2025-3-79-90

УДК 327; 323/324

Ладислав ЗЕМАНЕК

Секьюритизация в Европейском союзе (на примере Чехии)

Аннотация. В статье на примере Чешской Республики исследуется феномен секьюритизации в Евросоюзе. Подход, в рамках которого «интересы безопасности» ставятся выше демократических ценностей, гражданских свобод и иных соображений, больше не ограничивается традиционной военно-политической сферой, распространяясь на экономику, информацию, образование, науку и культуру. Под влиянием геополитической конфронтации, в первую очередь с Россией и Китаем, и предписаний Европейской комиссии, правительство Чехии институционализовало эту тенденцию посредством законодательных изменений, механизмов надзора, ограничений на экономическое взаимодействие и академическое сотрудничество. Делается вывод о том, что комплексная секьюритизация отражает парадоксальную эволюцию либеральной демократии к авторитарному управлению и снижению политической прозрачности.

Ключевые слова: секьюритизация, Евросоюз, рекомендации Еврокомиссии, Чехия, правительство П. Фиалы, безопасность, конфронтация, ограничения гражданских свобод, либеральная демократия, авторитарная эволюция.

Одним из ведущих трендов в политике Европейского союза является так называемая секьюритизация, подразумевающая приоритет «интересов безопасности» над всеми иными принципами и соображениями. Регламентация самых разных сфер — не только традиционных направлений обеспечения национальной безопасности, но и экономики, информации, образования, науки, культуры, гуманитарных контактов и т.д. — проникается дискурсом на тему угроз безопасности и политизированным видением, в основу которого положено противопоставление «демократий» и «автократий» как фундаментального разделительного рубежа современного мира.

Причины этого явления не сводятся к кризису европейской безопасности на почве конфронтации Запада с Россией и украинского конфликта в частности. Оно связано с общей трансформацией международного порядка и новым этапом глобальной конкуренции, подъемом крупных незападных держав, кризисом западного доминирования, с тенденцией к фрагментации, а точнее — регионализации мира, идущей на смену всеобщей глобализации. Правящие неолиберальные элиты, столкнувшись с систем-

Сведения об авторе: Ладислав ЗЕМАНЕК — научный сотрудник China-CEE Institute при Академии общественных наук КНР (Венгрия), доктор философии, zemanek.ml@gmail.com.

ными альтернативами как на международном уровне, так и внутри своих стран, пытаются удержать монопольное положение и собственные привилегии. Отсюда — курс на «секьюритизацию» экономических связей с «автократиями», нарративы «расцепления» и «дерискинга»; ужесточение контроля над инфраструктурной, информационной, идеологической, культурной, гуманитарной и др. сферами. Все это сочетается с резким увеличением оборонных бюджетов, вложениями в военно-промышленный комплекс (ВПК) и конфронтационной стратегией силового противостояния альтернативным игрокам.

От дискурса гибридной войны и кибербезопасности к всеобъемлющей секьюритизации

Традиционно проблематика безопасности и ее обеспечения ассоциировалась главным образом со сферами оборонной / военной стратегии, вооруженных сил, разведки и контрразведки, а также военно-политических союзов. Во всяком случае, тема безопасности не имела прямого определяющего влияния на большинство других общественных сфер. Ситуация стала меняться с появлением концепции гибридной войны, которая к середине 2010-х годов вышла на первый план официальной политической повестки НАТО. Дискурс гибридной войны создал концептуальный и психологический фон для неограниченной драматизации угроз, радикализировал общий дискурс безопасности и распространил его нарративы на сугубо гражданские области. Заметной вехой на этом пути стал, в частности, Варшавский саммит НАТО 2016 г., дополнивший наземные, военно-морские и воздушные оперативные сферы киберпространством.

С этого времени в Чехии (где первый закон о кибербезопасности был принят в 2014 г.) начались институциональные нововведения, затронувшие как военный, так и гражданский сектор. Начиная с 2017 г. возникла целая система соответствующих институтов: Национальное агентство кибер- и информационной безопасности (NUKIB / NCISA) в качестве головного административного ведомства в области кибербезопасности; Центр по борьбе с терроризмом и гибридными угрозами (CATHT) при чешском МВД; Комитет по кибербезопасности при Совете национальной безопасности; должность Специального представителя МИД по вопросам устойчивости и новых угроз; армейское Командование кибервойск и другие.

Все эти ведомства сформировали институциональную и нормативную базу «высокосекьюритизированного» всеобъемлющего дискурса гибридной войны. В «Стратегии кибербезопасности», принятой в 2020 г., устанавливались следующие приоритеты: разработка целостного подхода к кибербезопасности, основанного на гражданско-военном сотрудничестве; повышение устойчивости стратегической информационной инфраструктуры и систем управления; развитие основанного на единых ценностях международного сотрудничества в области кибербезопасности; взаимосвязь гражданского и военного секторов и создание совместной правовой базы евроатлантического киберпространства и т.п. [National Cyber Security Strategy...]

Следует отметить, что все разработанные в этой сфере программные документы, в том числе опубликованная в декабре 2021 г. «Национальная стратегия противодействия гибридному вмешательству» [National Cyber Security Strategy...], опираются на стратегические документы НАТО и ЕС, постулируя прежде всего неделимость чешской и евроатлантической безопасности — в согласии с основополагающей «Стратегией безопасности Чешской Республики».

Гибридное вмешательство связывается исключительно с действиями против западных либеральных демократий, которые, как утверждается, сталкиваются с угрозами «подрыва или срыва» в них демократических процессов, верховенства права и безопасности. В «Стратегии безопасности Чешской Республики» (2021) говорится, что атакам наиболее часто подвергаются, помимо инфраструктуры безопасности и обороны, ценности либерально-демократической системы и экономика. Всеобъемлющая политика противодействия гибридным угрозам, согласно документу, предполагает в том числе развитие возможностей адекватного и своевременного реагирования, публичное выявление лиц, совершающих гибридные преступления, и снижение зависимости от стран с «иными идеологическими и ценностными системами».

Принятая Чехией (и ЕС в целом) концепция кибербезопасности строится на принципах «нулевой суммы», исключительности западных либеральных демократий и их противопоставления «недемократическим» режимам, с которыми аксиоматически отождествляются все киберугрозы и риски. Такова и философия Пражских конференций по кибербезопасности, ежегодно организуемых NUKIB с участием представителей НАТО, США и европейских стран, а также «единомышленников» из Азии, включая Тайвань. Именно на первом из этих форумов в 2019 г. были одобрены поддержанные затем Большой семеркой «Пражские предложения» [The Prague Proposals], которые определили рекомендации по политике кибербезопасности в глобальном масштабе и стали отправной точкой для многих документов в этой области в разных странах.

Самоабсолютизация современной либеральной демократии и политизированный дискурс гибридной войны против нее парадоксальным образом ведут ее саму к антилиберальной и антидемократической эволюции. Показательно, что последние редакции «Стратегии безопасности Чешской Республики» включают в категорию серьезных угроз критику либерально-демократической модели, независимо от того, исходит ли эта критика со стороны внешних или внутренних субъектов [См. напр.: Security Strategy...2015].

Проблема такого подхода заключается в том, что он по сути делегитимирует свободу мысли и слова, идейный плюрализм, внутривнутриполитическую дискуссию, открытость к международному обмену — то есть то, что составляло фундаментальные черты самой либерально-демократической системы. Отныне любая внутренняя критика официального мейнстрима легко может быть расценена как действия в пользу внешних противников и гибридная угроза, что оказывает сильное давление на политическую оппозицию и гражданское общество во всех его сегментах, от административных

и бизнес-кругов до деятелей культуры, медийного, научно-экспертного и других сообществ.

Неотъемлемой стороной европейской политики секьюритизации становится противодействие избирательно определяемому «иностранному влиянию» во всех сферах общественной жизни. В некоторых областях, включая образование и науку, такой курс уже частично институционализирован. Об этом свидетельствуют создание должностей «менеджеров по безопасности» в ряде европейских (в том числе чешских) университетов, введение механизмов проверки, сокращение проектов сотрудничества с коллегами из «автократических» государств, ужесточение контроля и надзора за научными сотрудниками, преподавателями и студентами.

Новые законопроекты правительства П. Фиалы

Тенденция к всеобъемлющей секьюритизации усилилась в Чехии с приходом к власти в конце 2021 г. коалиционного правительства во главе с П. Фиалой. Аппарат безопасности и разведки активизировал усилия по внедрению принципа «безопасность превыше всего» в гражданские сферы — от производственного бизнеса и торговли до информации, образования и науки. Отдельные аспекты этой политики уже рассматривались нами в ряде публикаций [См. Напр.: Zemánek. Securitisation...].

В 2024 г. МВД и Национальное агентство кибер- и информационной безопасности Чехии подготовили и внесли в парламент очередные законопроекты — соответственно, о критической инфраструктуре и о кибербезопасности. Принятые в 2025 г., эти законы предусматривают внедрение обширных механизмов проверки для обеспечения «безопасных» цепочек поставок и исключения «рисков». Они серьезно скажутся на развитии таких отраслей, как энергетика, транспорт, информационно-коммуникационный сектор (ИКТ), финансы и банковское дело.

Доступ на чешский рынок экономических субъектов из идеологически неблизких стран существенно ограничивается. В последние годы объектом наиболее жестких рестрикций стал российский бизнес, причем эта практика началась еще до военной операции Москвы на Украине (например, консорциум с участием Росатома, как, впрочем, и китайские компании, не был допущен к тендеру на строительство нового энергоблока АЭС «Дукованы» [См. также: Задорожнюк. Провокация во Врбетице...]). Теперь в Праге вознамерились нанести решительный удар по позициям крупных китайских корпораций, в первую очередь Huawei (давнего партнера многих известных чешских компаний, включая Vodafone, T-Mobile и ČEZ), а также ZTE, Hikvision и Dahua [Sedlák]. Чешские органы безопасности еще в прошлом десятилетии были главной движущей силой кампании против стратегического партнерства с Пекином, в том числе и в экономической области. Они давно лоббируют ограничительный подход, предостерегая от китайских телекоммуникационных компаний, производителей видеооборудования и электромобилей, а также социальных сетей. По признанию высокопоставленных чешских чиновников, страны Запада, включая Чехию, рано или поздно введут общий запрет на определенные китайские технологии [Zelenka].

Следует отметить, что новый закон о кибербезопасности был разработан в порядке реализации Директивы NIS2 Европейской комиссии, принятой в конце 2022 г. [Directive (EU) 2022/2555]. Этот документ европейского права резко расширил требования к частным субъектам по внедрению мер безопасности, а также круг охватываемых организаций и секторов и обязал государства-члены ЕС адаптировать национальные законодательства к новым «стандартам кибербезопасности». Количество чешских юридических лиц, подпадающих под действие соответствующего регулирования, должно возрасти в 15 раз, примерно до 6 тыс. (вместо порядка 400), причем выполнение новых требований потребует от них огромных финансовых и кадровых ресурсов [NÚKIB sent...]. Кроме того, значительно расширятся запретительные полномочия Национального агентства кибер- и информационной безопасности. На фоне широкой негативной реакции в стране на этот законопроект Чешская торгово-промышленная палата и ряд компаний призвали правительство к его пересмотру.

Кабинет П. Фиалы также инициировал изменения в законе о защите страны. Прежде всего, было дано новое определение объектов, имеющих важное значение с точки зрения обороны и безопасности. До недавних пор круг таких стратегических объектов ограничивался особыми военными зонами, число которых сократилось до четырех (Болетице, Бржезина, Градиште и Либава). Объекты за их пределами не подпадали под действие данного закона, а различные военные объекты нередко возводились на участках земли, находящихся в частной собственности. По утверждению министерства обороны, некоторые «чувствительные» участки пытались купить иностранные граждане, что поставило бы под угрозу интересы национальной безопасности. На этом основании правительство провело поправку в закон, которая уполномочивает государственные органы выкупать либо даже экспроприировать участки, имеющие стратегическое значение для обороны страны, независимо от того, находятся ли они в специальных военных зонах или нет.

Как подчеркивали в оборонном ведомстве, законодательные изменения должны позволить увеличить мощности складов боеприпасов. (Запланировано расширение как минимум четырех из восьми государственных складов боеприпасов.) При этом с большой вероятностью встанет деликатный вопрос экспроприации частной собственности. Хотя чешская Конституция допускает использование данного правового инструмента во имя общественных интересов, до сих пор это было крайне затруднено. Законодательство, сложившееся после падения коммунистического режима, отдавало явный приоритет защите индивидуальных прав и конкретных частных интересов. Теперь следует ожидать смещения баланса в противоположную сторону и расширения практики экспроприации частной собственности.

Кроме того, секьюритизация уже привела к снижению прозрачности и затруднению общественного контроля в области политических решений и деятельности государственных инстанций в целом. Например, министерство обороны Чехии перестало предоставлять конкретную информацию о военной технике и закупках, ссылаясь на соображения безопасности. Ограничения на гласность государственных решений вышли

и далеко за рамки оборонной сферы: так, правительство П. Фиалы не опубликовало официальные доклады о пересмотре отношений с Россией и Китаем — одним из внешнеполитических приоритетов либеральной коалиции. Информация, связанная с подготовкой бюджета на 2025 г., также скрывалась — не только от общественности, но и от парламентской оппозиции. Для посткоммунистической Чехии подобная непрозрачность действий власти беспрецедентна. Отсутствие прозрачности критикуется оппозицией как «правительственная цензура» и вызывает негативную реакцию в чешском обществе [Wirnitzer. Nákupe...].

Проверка инвестиций и экономическая безопасность

Одним из инструментов политики секьюритизации (как на национальном уровне, так и на уровне Евросоюза) является механизм проверки и отбора иностранных инвестиций.

Европейская комиссия представила первую рамочную программу ЕС по проверке инвестиций в 2017 г. К тому моменту некоторые государства-члены уже внедрили свои национальные механизмы. К 2025 г. 24 из 27 стран-членов ЕС имели механизм проверки иностранных капиталовложений на национальном уровне, исключение составили Хорватия, Кипр и Греция. При этом действующие на пространстве Евросоюза правовые нормы в этой области различаются от страны к стране, что, по мнению сторонников секьюритизации, может снизить эффективность инструмента. Механизм фильтрации инвестиций является частью стратегии экономической безопасности, на растущем значении которой настаивают брюссельские инстанции.

Что касается Чехии, то в «Национальной стратегии противодействия гибридному вмешательству» 2021 г. поставлена, среди прочего, задача разработки эффективных механизмов проверки иностранных инвестиций. На практическом уровне скрининг инвестиций был введен в том же 2021 г. Он применяется в отношении иностранных инвесторов в тех случаях, когда конечный бенефициарный владелец средств находится за пределами ЕС. Обычно проверке подлежат капиталовложения, составляющие не менее 10% акций чешской компании, ведущей деятельность в том или ином секторе, который считается важным для национальной безопасности. Более строгие правила действуют в отношении инвестиций в производство военного оборудования и определенных товаров двойного назначения, а также в критическую инфраструктуру.

Согласно ежегодному отчету министерства промышленности и торговли, в 2023 г. государственные органы Чехии задействовали механизм проверки в 28 случаях против 13 случаев в 2022 г. [Výroční zpráva...]. Увеличение было связано по большей части с ростом числа «консультаций», то есть предварительной добровольной проверки на предмет возможных рисков для национальной безопасности либо конституционного и общественного порядка. Случаев наложения запрета на иностранные вложения в 2023 г. не было. На уровне ЕС доля запретов, наложенных на иностранные инвестиции, составила 1% от всех проверок. Большинство инвесторов в чешскую экономику,

попавших под проверку, были из США и Люксембурга, при этом конечные бенефициары находились в США и на Тайване. Что касается сфер предпринимательства, то в Чехии чаще всего проверялись капиталовложения в электротехническую отрасль, ИКТ и здравоохранение, а в ЕС в целом — в обрабатывающую промышленность и ИКТ.

В октябре 2023 г. Европейская комиссия определила десять технологических областей, критически важных с точки зрения безопасности:

- высокотехнологичные полупроводники;
- искусственный интеллект;
- квантовые технологии;
- биотехнологии;
- передовые средства связи, навигация и цифровые технологии;
- передовые сенсорные технологии;
- космос и двигатели;
- энергетика;
- робототехника и автономные системы;
- современные материалы, технологии производства и переработки [Commission Recommendation...].

Повестка экономической безопасности предполагает в этих областях как ужесточение контроля за экспортом, так и усиленный контроль над иностранными инвестициями. Кроме того, можно ожидать давления с целью включения в этот список иных категорий, например, «чистых технологий», что еще больше подстегнет тренд к избирательному «расцеплению» (decoupling) и «дерискингу» (derisking)¹ во внешнеэкономической политике [Demarais].

Секьюритизация в академическом секторе

Нарратив ограничения («безопасности») международного обмена в сфере науки и образования громко звучит в Евросоюзе как минимум с прошлого десятилетия. В Чехии, да и ряде других стран ЕС, сотрудничество с российскими академическими учреждениями и коллегами стало если не невозможным, то связанным с административными трудностями и карьерными рисками уже к началу 2020-х годов, еще за несколько лет до военной операции России на Украине, — будь то из-за ведомственных предписаний или активности ангажированных НПО, медийной травли и т.п. [см.: Zemánek. Securitisation...].

В государственной политике секьюритизации академического сектора официальная Прага выступила впереди большинства своих партнеров по ЕС. Реструктуризация на этом направлении началась в 2021 г., когда министерство внутренних дел выпустило «Руководство по противодействию иностранному влиянию для чешских высших учебных заведений».

1 Термин «дерискинг» (derisking) ввела в оборот глава Еврокомиссии У. фон дер Ляйен, говоря в марте 2023 г. об отношениях с Китаем.

Данный документ исходил из тезиса, что чешские университеты и ученые являются целями «воздействия из-за рубежа» и что они недостаточно защищены от внешнего влияния. Ссылаясь на опыт США и Великобритании, МВД Чехии предостерегало академическое сообщество от сотрудничества с коллегами и учреждениями из «авторитарных» стран, особенно России, Китая и Ирана, и призывало преподавателей и студентов сообщать администрации университета либо органам безопасности о контактах с представителями этих государств [Protivlivový manuál...].

В том же 2021 г. появилось подготовленное аналитическим управлением министерства финансов «Руководство по технической помощи и нематериальной передаче технологий», содержавшее еще более радикальные положения. В нем, в частности, определялись области, закрытые для изучения гражданами определенных стран. Аналогичные запреты устанавливались и на зарубежное сотрудничество образовательных и научных организаций [Příručka technické pomoci...].

С началом военных действий российской армии на Украине в 2022 г. практически все европейские университеты и научные центры прекратили отношения с российскими партнерами. Схожая тенденция, несмотря на формально иной контекст, наблюдается и в отношении Китая. Чешская академия наук и растущее число университетов Чехии принялись свертывать совместные проекты с китайскими коллегами, переориентируясь под влиянием курса официальной Праги на тайваньских партнеров.

Точкой отсчета качественно нового этапа в секьюритизации академической сферы на уровне Евросоюза можно считать май 2024 г., когда Совет ЕС по предложению Еврокомиссии принял «Рекомендацию по укреплению безопасности научных исследований» [Council Recommendation...]. Такое укрепление определяется как управление рисками, связанными с нежелательной передачей критически важных знаний и технологий, злонамеренным влиянием со стороны третьих стран либо в их интересах, а также нарушениями этики и «целостности», когда знания и технологии используются для нанесения ущерба фундаментальным «правам и ценностям» Евросоюза. Документ прямо ссылается на опубликованную в июне 2023 г. Европейскую стратегию экономической безопасности, которая отводит одну из ключевых ролей исследованиям и инновациям, а также на вышеупомянутый перечень десяти технологических областей, критически важных для безопасности и стратегической автономии ЕС.

Фактически секьюритизация подразумевает подчинение сферы науки и высшего образования задачам геополитики и международной конфронтации. Европейские власти используют концепцию гибридных угроз, чтобы, апеллируя к соображениям безопасности, подчинить научные исследования своим политическим интересам и наложить ограничения на профессиональное сотрудничество европейских академических кругов с коллегами из «автократических» стран.

Важно, что к прежним, часто неформальным, методам давления и контроля добавляется институционализация «исследовательской безопасности» посредством взаи-

модействия университетов и научных учреждений со спецслужбами. Принятая в мае 2024 г. рекомендация ЕС призвала вовлечь в экосистему исследований и инноваций такие инстанции, как Единый аналитический центр разведки (SIAC), Европейский центр передового опыта по противодействию гибридным угрозам (Hybrid CoE), Агентство ЕС по кибербезопасности (ENISA) и Европейский центр по киберпреступности (EC3).

Предусмотрено создание механизмов официального сотрудничества научных организаций со спецслужбами и подобными инстанциями. Совет ЕС заключил, что обмен информацией между исполнителями и спонсорами исследований, с одной стороны, и представителями разведки и контрразведки, с другой, должен осуществляться посредством закрытых и открытых брифингов, а также через «офицеров связи» в исследовательских центрах и университетах. Кроме того, была отмечена необходимость укреплять соответствующее взаимодействие в системе государственного управления и правительственных органов путем межведомственной координации действий высокопоставленных чиновников, отвечающих за высшее образование, исследования и инновации, торговлю, внешнюю политику, разведку и безопасность. Данные предписания явно направлены в первую очередь против Китая, поскольку правящие круги Евросоюза все больше опасаются влияния КНР на европейские дела, в том числе по каналам передачи знаний и технологий [Наеск].

Все эти инструменты контроля постепенно внедряются в Чешской Республике. В июне 2024 г. чешское министерство образования, со своей стороны, представило инструкции по укреплению «устойчивости против нелегитимного влияния» в области образования и науки.

Следствиями «секьюритизированного» подхода к научно-образовательной политике стали: распространение атмосферы недоверия и подозрений; усиление цензуры и самоцензуры; исключение из академического процесса (либо маргинализация) ряда учебных курсов, научных тем и концепций; административные наказания ученых и преподавателей с альтернативными взглядами; их публичная диффамация в СМИ и социальных сетях.

Парадоксально, что руководящие органы государств-членов ЕС и сами брюссельские инстанции не признают эти ограничения и репрессивные меры нарушениями академических прав и свобод. В то же время стандартное профессиональное сотрудничество с коллегами из так называемых авторитарных стран, к которому чаще всего сводится «влияние иностранной державы», расценивается как серьезное нарушение этих самых академических прав и свобод.

Изменения в Уголовном кодексе

Однако все директивы о «секьюритизации» и дискриминация инакомыслия в академической среде меркнут на фоне поправок к Уголовному кодексу Чешской Республики, которые в ноябре 2024 г. получили одобрение кабинета министров и были приняты

в феврале 2025 г. Правительство П. Фиалы и поддерживающая его либеральная коалиция согласились с настойчивым требованием службы контрразведки провести новый уголовный закон, который в определении шпионажа выходит далеко за рамки действующего законодательства.

До сих пор Уголовный кодекс предусматривал наказание за несанкционированное использование секретной информации в пользу иностранного субъекта. Новая поправка существенно расширяет сферу уголовно наказуемых действий, распространяя ее как на секретную, так и на несекретную информацию. Правительство утвердило положение о том, что чешский гражданин, осуществлявший деятельность в пользу иностранного субъекта в ущерб национальной безопасности и интересам соответствующих международных организаций, может быть приговорен к тюремному заключению сроком до 12 лет. Согласно новой поправке, наказуемой является уже подготовка к такой деятельности, причем государственные органы не будут принимать во внимание, осуществляется ли она в Чехии или за рубежом [Zákon, kterým... Svorník]. Такие изменения в Уголовном кодексе предоставят спецслужбам и аппарату безопасности беспрецедентные полномочия. Например, они позволят преследовать и наказывать за практически любые формы сотрудничества или контактов с иностранными субъектами из так называемых автократических стран. Бывший президент Чехии М. Земан назвал данную поправку в УК «тоталитарным инструментом», что резонирует с давно звучащими предостережениями политической оппозиции против опасности возникновения либерального «нового тоталитаризма» [Panenka; Rambousková, Gavenda, Machová].

* * *

Как показывает проведенный анализ, распространение дискурса безопасности на различные общественные сферы — это долгосрочная тенденция, усилившаяся в последний период, особенно в связи с концепцией гибридной войны и нарастанием глобальной конкуренции. Всеобъемлющая секьюритизация ведет к капитальным политическим, экономическим и социальным последствиям.

Расширительное и произвольное, политически и идеологически мотивированное, толкование безопасности ставит под угрозу основные права и гражданские свободы, налагая все большие ограничения на индивидуумов и общественные субъекты. Более того, подчинение экономического, культурного, академического обмена, гуманитарных контактов такому дискурсу безопасности подрывает нормальные прагматичные отношения с внешним миром, поскольку создает разделительную линию между идеологически близкими странами, с одной стороны, и так называемыми врагами и соперниками, с другой.

Происходящие в этом русле сдвиги в Чехии и во всем Европейском союзе свидетельствуют о парадоксальной трансформации западной либеральной демократии в направлении авторитаризма и закрытости.

Литература

- Задорожнюк Э.* Провокация во Врбетице: опасные повороты чешской нанополитики // Перспективы. Электронный журнал. 2021. №2/3. С. 129-140. — URL: perspektivy.info/upload/iblock/d16/2_3_2021_0_129_140.pdf (date of access: 03.09.2025).
- Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States. 11.10.2023. — URL: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302113 (date of access: 03.09.2025).
- Council Recommendation on Enhancing Research Security. Brussels. 14.05.2024. — URL: data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf (date of access: 03.09.2025).
- Demarais A.* What the EU list of critical technologies tells us about its de-risking plans // European Council on Foreign Relations. 11.10.2023. — URL: ecfr.eu/article/what-the-eu-list-of-critical-technologies-tells-us-about-its-de-risking-plans/ (date of access: 03.09.2025).
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022// EUR-Lex. — URL: eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng (date of access: 03.09.2025).
- Haack P.* EU wants spies on university campuses to fight Chinese tech espionage // Politico. 23.05.2024. — URL: politico.eu/article/academic-research-campus-eu-universities-intelligence-services-china-spying-technology/ (date of access: 03.09.2025).
- National Cyber Security Strategy of the Czech Republic. Prague. 2020. — URL: dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/nscs_2021_2025_eng.pdf (date of access: 03.09.2025).
- NÚKIB sent a draft proposal of the new law on cyber security to the Government Legislative Council // NÚKIB. 03.01.2024. — URL: nukib.gov.cz/en/infoservis-en/news/2065-nukib-sent-a-draft-proposal-of-the-new-law-on-cyber-security-to-the-government-legislative-council/ (date of access: 03.09.2025).
- Panenska R.* Zeman: Fiala připomíná Hitlera v bunkru. BIS se chystá zatýkat // ParlamentníListy.cz. 20.11.2024. — URL: parlamentnilisty.cz/arena/rozhovory/Zeman-Fiala-pripomina-Hitlera-v-bunkru-BIS-se-chysta-zatykat-765127 (date of access: 03.09.2025).
- Příručka technické pomoci a nehmotného přenosu technologií. Prague. 2021. Aktualizováno v prosinci 2024. — URL: fau.gov.cz/files/prirucka-technicke-pomoci-v2024-final.pdf (date of access: 03.09.2025).
- Protivlivový manuál pro sektor vysokých škol // Centrum proti hybridním hrozbám. — URL: mv.gov.cz/chh/clanek/protivlivovy-manual-pro-sektor-vysokych-skol.aspx (date of access: 03.09.2025).
- Rambousková M., Gavenda J., Machová M.* Nová totalita je tu, hájí Babiše jeho poslanci v předvečer 17. listopadu // Seznam Zprávy. 16.11.2023. — URL: seznamzpravy.cz/clanek/domaci-politika-nova-totalita-je-tu-haji-babise-jeho-poslanci-v-predvecer-17-listopadu-239839 (date of access: 03.09.2025).
- Security Strategy of the Czech Republic. Prague. 2015. — URL: mzv.gov.cz/public/2a/57/16/1375879_1259981_Security_Strategy_CZ_2015.pdf (date of access: 03.09.2025).
- Sedlák J.* Také vnitro chce zakazovat dodavatele do kritické infrastruktury. Dřímají v ní rizikové kamery z Číny // Lupa.cz. 17.04.2024. — URL: lupa.cz/clanky/take-vnitro-chce-zakazovat-dodavatele-do-kriticke-infrastruktury-drimaji-v-ni-rizikove-kamery-z-ciny/ (date of access: 03.09.2025).

- Svorník P.* Nový trestný čin: Za sběr dat pro cizí mocnost až 12 let vězení // Novinky.cz. 18.11.2024. — URL: novinky.cz/clanek/domaci-novy-trestny-cin-za-sber-dat-pro-cizi-mocnost-az-12-let-vezeni-40497777 (date of access: 03.09.2025).
- The Prague Proposals. The Chairman Statement on cyber security of communication networks in a globally digitalized world. Prague 5G Security Conference. Prague, 3 May 2019. — URL: vlada.gov.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf (date of access: 03.09.2025).
- Výroční zpráva o prověřování zahraničních investic v České republice za rok 2023. Ministerstvo průmyslu a obchodu. 10.12.2024. — URL: mpo.gov.cz/assets/cz/zahranicni-obchod/proverovani-zahranicnich-investic/2024/12/vyrocní_zprava23_1.pdf (date of access: 03.09.2025).
- Wirnitzer J.* Nákupy bez „jakékoli kontroly“? Co a proč už ministerstvo obrany nechce zveřejňovat // Deník N. 26.01.2024. — URL: denikn.cz/1332436/nakupy-bez-jakekoli-kontroly-co-a-proc-uz-ministerstvo-obrany-nechce-zverejnovat/ (date of access: 03.09.2025).
- Zákon, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 141/1961 Sb... // ODok. — URL: odok.cz/portal/veklep/material/KORND3QJZZZ3/ (date of access: 03.09.2025).
- Zelenka F.* Směřujeme k zákazu některých čínských technologií, říká český kyberzmocněnec // E15. 20.04.2024. — URL: e15.cz/byznys/technologie-a-media/smerujeme-k-zakazu-nekterych-cinskych-technologie-rika-cesky-kyberzmocnenec-1415061 (date of access: 03.09.2025).
- Zemánek L.* Securitisation of the Social Sphere: Synchronic and Diachronic Perspective // Weekly Briefing. Vol. 46. No. 3 (CZ) December 2021. — URL: china-cee.eu/2022/01/11/czech-republic-social-briefing-securitisation-of-the-social-sphere-synchronic-and-diachronic-perspective/#_ftnref5 (date of access: 03.09.2025).