ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ БЕЛАРУСИ И СТРАН ЕВРОПЕЙСКОГО СОЮЗА

Шерышев Р.В., студент гр. 561402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пухир Г.А. – старший преподаватель каф. ЗИ

Аннотация. В работе рассматриваются подходы к регулированию деятельности организаций в сфере защиты информации в Республике Беларусь и странах Европейского Союза. Анализируется белорусская модель лицензирования, основанная на разрешительном принципе, а также европейская практика аккредитации и надзора, применяемая при работе с государством и критической инфраструктурой. Выявляются ключевые различия между двумя системами: лицензированием как обязательным условием осуществления деятельности в Беларуси и дифференцированным подходом в странах ЕС.

Ключевые слова. Регулирование деятельности, скрытность передачи, ASK, FSK, BPSK, спектральная плотность мощности, PAPR, распознавание сигналов.

Информация в современных условиях превратилась в один из ключевых стратегических ресурсов, требующих надежной защиты. Деятельность по обеспечению информационной безопасности связана с высокой степенью ответственности, поскольку специализированные методы и средства защиты, оказавшись в распоряжении злоумышленников, могут быть использованы для нанесения ущерба критически важной инфраструктуре. В условиях трансграничного обмена данными особое значение приобретает анализ международных подходов к регулированию этой сферы. Сравнение белорусской модели лицензирования с европейскими механизмами сертификации, аккредитации и надзора позволяет выявить различные способы минимизации рисков, обусловленных двойственным характером знаний и технологий в области защиты информации.

В Республике Беларусь регулирование деятельности в сфере защиты информации исторически развивается на основе лицензирования, а также обязательной сертификации и аттестации средств и систем защиты информации. Формирование национальной системы законодательства о лицензировании началось с Постановления Совета Министров Республики Беларусь от 16 октября 1991 г. № 386. В настоящее время отношения в сфере лицензирования регулируются Законом Республики Беларусь от 14 октября 2022 г. № 213-З «О лицензировании», который определяет общие подходы к лицензируемым видам деятельности и порядок их осуществления. Вопросы, связанные с деятельностью в области защиты информации, дополнительно регулируются Указом Президента Республики Беларусь от 16 февраля 2012 г. № 71 «О порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами)», устанавливающим особенности лицензирования деятельности, связанной с криптографической защитой информации и средствами негласного получения информации.

Лицензирование деятельности по технической и криптографической защите информации, включая применение электронной цифровой подписи, осуществляет Оперативно-аналитический центр при Президенте Республики Беларусь. В части средств криптографической защиты государственных секретов и средств негласного получения информации соответствующие полномочия возложены на Комитет государственной безопасности.

В Европейском союзе отсутствует единое обязательное государственное лицензирование всей деятельности по защите информации. Регулирование осуществляется через сочетание сертификации, стандартов, национального надзора и общеевропейских нормативных актов, прежде всего GDPR и NIS2. GDPR устанавливает правила обработки персональных данных для организаций, работающих с данными граждан ЕС, независимо от места их нахождения. Он предусматривает обязанности по назначению ответственного за защиту данных в предусмотренных случаях, проведению оценки рисков и внедрению мер безопасности, но не требует получения обязательной государственной лицензии.

Директива NIS2, принятая в 2022 году, усилила требования к кибербезопасности организаций в критически важных секторах ЕС, включая энергетику, транспорт, банковский сектор, здравоохранение и государственное управление. Она обязывает организации внедрять меры управления рисками, обеспечивать защиту цепочек поставок, поддерживать непрерывность деятельности и своевременно уведомлять о значимых инцидентах. В ряде случаев предусмотрена и повышенная ответственность руководства за соблюдение требований кибербезопасности. [1]

Деятельность по защите информации также опирается на международные стандарты, в частности на:

ISO/IEC 27001:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования»;

ISO/IEC 27002:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление информационной безопасностью»;

ISO/IEC 27005:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по управлению рисками информационной безопасности».

В государствах ЕС существуют национальные особенности регулирования защиты информации, обусловленные историческими, управленческими факторами и требованиями национальной безопасности. Общим принципом является дифференциация требований в зависимости от статуса организации и характера обрабатываемых данных. Для коммерческих компаний, не связанных с госорганами и критической инфраструктурой, обязательное получение разрешений в сфере информационной безопасности обычно не требуется; их деятельность регулируется GDPR и NIS2. Обязательная аккредитация, сертификация или признание со стороны национального регулятора необходима при работе с госзаказчиками, объектами критической инфраструктуры или особо чувствительными данными. Однако в отдельных странах такие требования распространяются на криптографические средства и поставщиков, выполняющих государственные контракты. [2]

В Германии функции профильного регулятора выполняет Федеральное ведомство по информационной безопасности (BSI). Оно ведет механизмы признания и оценки компетентности поставщиков и решений в сфере ИТ-безопасности, а в отдельных случаях устанавливает дополнительные требования для работы с государственными структурами и операторами критической инфраструктуры. Для деятельности, связанной с криптографической защитой информации в государственных системах, могут применяться дополнительные процедуры согласования и аккредитации.

Во Франции головным органом выступает Национальное агентство безопасности информационных систем (ANSSI). Для работы с государственными заказчиками и в чувствительных секторах оно применяет механизмы квалификации и сертификации, подтверждающие техническую компетентность и надежность поставщиков. Криптографические продукты, предназначенные для защиты государственной информации, подлежат обязательной сертификации в установленном порядке.

В Нидерландах надзор в сфере информационной безопасности распределён между несколькими государственными структурами. Ключевую роль играет Национальный центр кибербезопасности (NCSC), который анализирует угрозы, координирует реагирование и даёт рекомендации по защите цифровой инфраструктуры. В сфере персональных данных действует Управление по защите данных (AP), контролирующее соблюдение GDPR. Обязательные процедуры признания, согласования или аккредитации, как правило, применяются прежде всего при работе с государственными органами и объектами критической инфраструктуры, тогда как коммерческий сектор в основном действует в рамках общеевропейского регулирования без дополнительных административных барьеров.

В Испании ключевую роль играет Национальный криптологический центр (CCN), который связан с формированием и применением требований к безопасности информационных систем в государственном секторе. Каталог продуктов и услуг безопасности (CPSTIC) используется как ориентир при выборе средств защиты информации для государственных органов и объектов критической инфраструктуры. Для систем, работающих с информацией ограниченного распространения, применяется Национальная схема безопасности (ENS), а сертификация соответствия осуществляется через уполномоченные и аккредитованные органы.

В Польше национальная система регулирования строится вокруг Закона о национальной системе кибербезопасности (UKSC), который устанавливает требования для операторов ключевых сервисов и объектов критической инфраструктуры. Надзорные функции распределены между несколькими государственными институтами: Научно-академическая компьютерная сеть (NASK) участвует в координации и технической поддержке, Агентство внутренней безопасности (ABW) играет важную роль в вопросах государственной и криптографической безопасности, а Министерство национальной обороны отвечает за оборонный сектор.

Проведенный анализ показывает принципиальные различия в подходах к регулированию деятельности в сфере защиты информации в Республике Беларусь и Европейском союзе. Белорусская модель строится на более централизованном государственном контроле, где лицензирование, сертификация и аттестация выступают ключевыми механизмами допуска к деятельности. Европейская модель, напротив, основана на стандартизации, последующем надзоре и усиленной ответственности без единой системы обязательного лицензирования. Выбор той или иной модели определяется национальными приоритетами: в первом случае акцент делается на государственную безопасность и контроль, во втором – на развитие рынка при высоких требованиях к соблюдению правил. В дальнейшем системы защиты информации, вероятно, будут все активнее сочетать элементы риск-ориентированного подхода, что позволит повысить устойчивость критической инфраструктуры в условиях роста глобальных киберугроз.

Список использованных источников:

1. Kianpour, M., Earls Davis, P.A. & Windekilde, I.M. Digital sovereignty in practice: analyzing the EU's NIS2 directive. Int. J. Inf. Secur. 24, 167 (2025)

2. Верхелст Э., Ваутерс Я. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций: образование, наука, новая экономика. 2020, Т. 15, № 2. – С. 105-124.