УДК 004.056.5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РЕСПУБЛИКЕ БЕЛАРУСЬ: ОТ КОНЦЕПЦИИ К ПРАКТИКЕ И ВЫЗОВАМ

Довыденко Иван Иванович,
Могилевский государственный университет имени А. А. Кулешова
(г. Могилев, Республика Беларусь)

В данной статье рассматривается понятие информационной безопасности с опорой на нормативно-правовую базу Республики Беларусь, проводится сравнительный анализ различных подходов к определению термина «информационная безопасность» на уровне хозяйствующих субъектов, а также выделяются основные проблемы, связанные с обеспечением информационной безопасности в стране.

В современном мире информационные технологии занимают ключевое место в обеспечении функционирования государственных институтов, бизнеса и общества в целом. В связи с этим информационная безопасность становится важнейшим элементом национальной безопасности. В Республике Беларусь вопросам информационной безопасности уделяется значительное внимание как на государственном уровне, так и на уровне хозяйствующих субъектов.

Информационная безопасность в Республике Беларусь рассматривается как элемент национальной безопасности, направленный на защиту информационных ресурсов, систем и процессов от внутренних и внешних угроз, обеспечивая тем самым устойчивое функционирование государства, общества и экономики.

Согласно Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 09.11.2010 № 575 (в ред. Указа Президента Республики Беларусь от 24.05.2023 № 145), информационная безопасность определяется как: «состояние защищенности национальных интересов Республики Беларусь в информационной сфере от внешних и внутренних угроз, обеспечивающее устойчивое развитие государства, реализацию конституционных прав и свобод граждан, а также эффективное функционирование информационных систем и ресурсов».

Это определение подчеркивает комплексный характер информационной безопасности, охватывающий не только технические аспекты защиты информации, но и более широкие социально-политические и экономические интересы государства и общества.

Ключевыми нормативно-правовыми актами, регулирующими вопросы информационной безопасности в Республике Беларусь, являются:

- Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации». Является базовым законом, определяющим правовые основы регулирования отношений в сфере информации, информатизации и защиты информации. Он устанавливает принципы защиты информации, права и обязанности субъектов информационных отношений, а также виды ответственности за нарушение законодательства в этой сфере.
- Указ Президента Республики Беларусь от 16 декабря 2019 г. № 467 «О мерах по обеспечению информационной безопасности». Данный Указ является одним из ключевых документов, определяющих стратегические направления и механизмы обеспечения информационной безопасности. Он утверждает Концепцию информационной безопасности Республики Беларусь, устанавливает основные принципы и приоритеты государственной политики в этой сфере.
- Постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 673 «О некоторых мерах по реализации Закона Республики Беларусь "Об информации, информатизации и защите информации"». Регулирует вопросы создания и функционирования государственных информационных систем, а также устанавливает требования к защите информации в них.
- Технические нормативные правовые акты (ТНПА): многочисленные стандарты, технические кодексы установившейся практики (ТКП) и государственные стандарты (СТБ), разработанные Государственным комитетом по стандартизации Республики Беларусь, детализируют требования к системам защиты информации, методам и средствам обеспечения информационной безопасности. Примеры включают СТБ ISO/IEC 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», ТКП 339-2011 «Информационные технологии. Защита информации. Общие положения».

На уровне хозяйствующих субъектов (предприятий, организаций, компаний) определение информационной безопасности, хотя и базируется на общих принципах, закрепленных в законодательстве, приобретает более прикладной и прагматичный характер. Здесь можно выделить несколько подходов, которые часто пересекаются и дополняют друг друга:

- Подход, ориентированный на защиту активов (Asset-centricapproach). Этот подход фокусируется на идентификации и защите информационных активов организации (данные, программное обеспечение, аппаратное обеспечение, информационные системы, репутация). Информационная безопасность определяется как состояние, при котором эти

активы защищены от несанкционированного доступа, использования, раскрытия, изменения, уничтожения или нарушения работоспособности. Основное внимание уделяется оценке стоимости активов и потенциального ущерба от их компрометации.

1. Подход, основанный на триаде CIA (Confidentiality, Integrity, Availability). Это классический и широко используемый подход, где информационная безопасность определяется через обеспечение трех ключевых свойств информации: конфиденциальность (Confidentiality), целостность (Integrity), доступность (Availability).

2. Подход, основанный на управлении рисками (Risk-basedapproach). В этом подходе информационная безопасность рассматривается как процесс идентификации, оценки, анализа и управления информационными рисками. Определение информационной безопасности сводится к минимизации вероятности реализации угроз и снижению потенциального ущерба до приемлемого уровня.

3. Подход, ориентированный на соответствие требованиям (Compliance-drivenapproach). Для многих хозяйствующих субъектов информационная безопасность определяется как соответствие требованиям законодательства, отраслевых стандартов и внутренних политик.

4. Подход, ориентированный на непрерывность бизнеса (Business Continuity-drivenapproach). В этом случае информационная безопасность тесно связана с обеспечением непрерывности бизнес-процессов. Она определяется как способность организации продолжать свою деятельность даже в условиях инцидентов информационной безопасности, минимизируя простои и потери.

На практике большинство хозяйствующих субъектов используют гибридный подход, комбинируя элементы всех вышеперечисленных, чтобы создать комплексную и эффективную систему информационной безопасности, адаптированную к их специфическим потребностям и рискам.

Несмотря на значительные успехи в формировании нормативно-правовой базы по информационной безопасности в Республике Беларусь, существуют определенные проблемы и вызовы, которые требуют дальнейшего внимания и совершенствования.

- Недостаточная детализация и актуализация некоторых нормативных актов. Хотя общие принципы и направления определены, некоторые подзаконные акты и технические нормативные правовые акты (ТНПА) могут отставать от быстро меняющихся технологий и угроз. Это приводит к тому, что организации сталкиваются с трудностями в интерпретации и применении требований, а также в выборе адекватных средств защиты.

- Проблема гармонизации с международными стандартами и лучшими практиками. Несмотря на наличие СТБ ISO/IEC 27001, не все белорусские стандарты полностью гармонизированы с международными. Это может создавать барьеры для белорусских компаний, работающих на международном рынке, и затруднять внедрение передовых мировых практик в области информационной безопасности.
- Недостаточное регулирование новых видов угроз и технологий. Быстрое развитие таких технологий, как искусственный интеллект, интернет вещей (IoT), облачные вычисления, квантовые вычисления, а также появление новых видов киберугроз (например, атаки на цепочки поставок, глубокие фейки), требует оперативного реагирования со стороны законодательства. Существующая нормативная база не всегда успевает за этими изменениями, оставляя пробелы в регулировании.
- Проблемы правоприменения и ответственности. Несмотря на наличие статей в Уголовном кодексе и Кодексе об административных правонарушениях, касающихся преступлений в сфере компьютерной информации, возникают сложности с доказыванием, квалификацией и привлечением к ответственности за киберпреступления, особенно трансграничные.
- Недостаточное регулирование вопросов киберстрахования. В мировой практике киберстрахование становится важным инструментом управления рисками информационной безопасности. В Республике Беларусь этот сегмент рынка находится на начальной стадии развития, и нормативно-правовая база, регулирующая его, пока недостаточно развита.
- Сложность и объемность нормативной базы. Для хозяйствующих субъектов, особенно малого и среднего бизнеса, ориентироваться в большом количестве законов, указов, постановлений, ТНПА может быть затруднительно. Это требует упрощения и систематизации нормативной базы, а также разработки понятных методических рекомендаций.
- Недостаточное стимулирование внедрения систем менеджмента информационной безопасности. Существуют стандарты, обязывающие внедрять системы защиты информации, не всегда есть достаточные стимулы для организаций к построению комплексных систем менеджмента информационной безопасности, основанных на риск-ориентированном подходе.

Решение этих проблем требует постоянного мониторинга, анализа и совершенствования нормативно-правовой базы, активного взаимодействия государства с бизнесом и экспертным сообществом, а также учета международного опыта.

Список использованных источников

1. Концепция национальной безопасности Республики Беларусь : утв. Указом Президента Респ. Беларусь, 09.11.2010, № 575 : в ред. Указа Президента Респ. Беларусь, 24.05.2023, № 145 / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025. – URL: http://www.pravo.by (дата обращения: 25.11.2025).
2. Об информации, информатизации и защите информации : Закон Респ. Беларусь, 10 ноября 2008 г., № 455-З : в ред. Закона Респ. Беларусь, 11.05.2023, № 268-З) / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025. – URL: http://www.pravo.by (дата обращения: 25.11.2025).
3. О мерах по обеспечению информационной безопасности : Указ Президента Респ. Беларусь, 16 декабря 2019 г., № 467 / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025. – URL: http://www.pravo.by (дата обращения: 25.11.2025.)
4. О защите персональных данных : Закон Респ. Беларусь, 7 мая 2021 г., № 90-З / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025. – URL: http://www.pravo.by (дата обращения: 25.11.2025).
5. СТБ ISO/IEC 27001-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025. – URL: http://www.pravo.by (дата обращения: 25.11.2025).
6. ТКП 339-2011 «Информационные технологии. Защита информации. Общие положения» / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025. – URL: http://www.pravo.by (дата обращения: 25.11.2025).