Пересмотрены правила функционирования национальной системы кибербезопасности

 Пересмотрены правила функционирования национальной системы кибербезопасности. Соответствующий приказ Оперативно-аналитического центра при Президенте Республики Беларусь опубликован на Национальном правовом Интернет-портале Республики Беларусь.

Ключевой принцип изменений – законодательство о кибербезопасности должно быть фактически выполнимым для всех участников национальной системы – от крупных центров кибербезопасности до небольших организаций, имеющих выход в интернет.

В числе главных изменений:
Классификация киберинцидентов: по масштабу последствий
Вводятся три уровня (вместо двух) киберинцидентов. Критерий – масштаб последствий.
Практическое правовое значение изменения: 19 июня 2026 года вступают в силу статьи 23.11 и 23.12 КоАП, устанавливающие административную ответственность в области обеспечения кибербеза, которая наступает только в случае возникновения киберинцидента высокого уровня.

 Документооборот с ОАЦ: принцип «разумной достаточности»
– Отменяется обязанность ЦКБ направлять в ОАЦ регламенты обеспечения кибербезопасности и планы мероприятий по реагированию на киберинциденты.
– Вводится отчетность (дважды в год) о результатах работы ЦКБ.

 Штат ЦКБ: обязательные специалисты
В штате ЦКБ, оказывающих услуги другим организациям, обязательно должны быть специалисты по анализу вредоносного программного обеспечения и специалисты по оценке эффективности защищенности.

Договоры на приобретение услуг по обеспечению кибербезопасности: корректировка существенных условий
Обязательные закупки услуг – по понятным и единообразным правилам, исключающим недобросовестное исполнение.

Аудит кибербезопасности и оценки защищенности: детальная регламентация процессов
Наиболее значимые по содержанию изменения. Их цель – чтобы заказчики, которые не обладают достаточными специальными компетенциями, не приобретали «кота в мешке» и могли объективно оценить качество полученных услуг.

 Порядок информационного взаимодействия с Национальным центром кибербезопасности
– Можно использовать электронную почту и телефонную связь. Главное – максимально быстро начать необходимые мероприятия.
– Предоставление информации о событиях кибербезопасности и киберинцидентах в иностранные или международные организации согласовывается с ОАЦ.

Порядок работы команд реагирования: стандартизация действий
– Обязательная фиксация мероприятий по реагированию на киберинциденты в системе обработки сведений о киберинцидентах.
– Сведения для выявления индикаторов компрометации должны сохраняться строго в соответствии с рекомендациями ОАЦ, которые будут размещены на сайте.

Изменения вступают в силу с 1 июля 2026 года

НЦКБ напоминает, что требования по кибербезопасности касаются каждой организации в Беларуси, так как для злоумышленников нет «неинтересных» объектов. Компрометация даже рядового объекта превращает его в инструмент атаки на объекты, относящиеся к национальной информационной инфраструктуре.

 Подробнее о нововведениях – в комментарии представителя Национального центра кибербезопасности в ближайшем номере журнала «Веснік сувязі»
