Влияние соответствия требованиям директивы NIS2 на конкурентоспособность предприятия 1/19/25

директор отдела ИТ-консалтинга, PwC
Латвия
Dr.dat. Baiba Apine

NIS2 (Network and Information Security Directive) – это директива Европейского союза, целью которой является укрепление кибербезопасности во всем ЕС, особенно в отношении критически важной инфраструктуры и значимых услуг. Латвия транспонировала данную директиву в национальное законодательство, приняв закон «О национальной кибербезопасности» (далее в тексте – ЗНК). В настоящий момент предприятиям необходимо определить свой статус (являются или не являются субъектом ЗНК) и до 1 апреля 2025 года зарегистрироваться в Национальном центре кибербезопасности (НЦК). Организации обязаны назначить руководителя по кибербезопасности и до 1 октября текущего года подать первый доклад по самооценке, а с 1 июля текущего года начать сообщать об инцидентах кибербезопасности.

В организованном компанией PwC опросе «Цифровая надежность – 2025», особое внимание в котором уделялось кибербезопасности, приняли участие более 4000 руководителей предприятий и руководителей по информационным технологиям из 77 стран. Лишь 2% руководителей сочли, что их предприятия приняли достаточные меры по киберустойчивости. Менее 50% респондентов указали, что их руководители по кибербезопасности участвуют в стратегическом планировании и подготовке докладов руководства предприятия. Это недвусмысленно указывает на то, что на практике в сфере кибербезопасности больше разговоров, чем дел.

Цель директивы NIS2 – силой закона принудить около 100 000 предприятий в ЕС укрепить киберустойчивость, усилить роль руководителя по кибербезопасности на предприятии и сократить угрозы. В Латвии ЗНК может затронуть около 1500 предприятий, в настоящий момент процесс регистрации в НЦК начали приблизительно 600 предприятий.

Внедрение NIS2 и ЗНК определенно не является шагом к сокращению бюрократии. Внедрение требований увеличит административное бремя предприятий, поскольку им потребуется разработать политику в сфере киберрисков, процедуры выявления инцидентов и сообщения о них, а также план обеспечения непрерывной деятельности. Однако закон вынуждает руководителей предприятий изменить отношение к кибербезопасности. Реализация требований NIS2 повысит киберустойчивость, но не гарантирует полную защиту от инцидентов. К примеру, реагирование на инциденты и планы обеспечения непрерывности деятельности помогают предприятиям быстро восстановиться после киберугроз. Улучшая защиту своих систем, сокращая риски утечки дорогостоящих данных и простоя, а также содействуя лояльности клиентов, предприятия окажутся в лучшем положении для партнерства и доступа к рынку ЕС.

Соответствие требованиям директивы NIS2 является важным шагом к укреплению кибербезопасности предприятий, и ее внедрение потребует активного участия всех вовлеченных сторон. Несмотря на то что административное бремя может вызвать сложности, предприятия, которые успешно реализуют требования директивы NIS2, будут лучше подготовлены к будущим

киберугрозам и смогут сохранить конкурентоспособность на рынке ЕС.