СОВЕТ
ПО РАЗВИТИЮ ЦИФРОВОЙ ЭКОНОМИКИ
ПРИ СОВЕТЕ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ул. Б. Дмитровка, д. 26, Москва,103426

___ _____2023 г. №_____

РЕШЕНИЕ

секции «Обеспечение технологического суверенитета и информационной безопасности Российской Федерации» Совета по развитию цифровой экономики при Совете Федерации Федерального Собрания Российской Федерации

18 мая 2023 года г. Москва

Согласно указу Президента Российской Федерации, переход на отечественное программное обеспечение (далее – ПО) на значимых объектах критической информационной инфраструктуры (далее – КИИ) должен быть осуществлен до 1 января 2025 года.

Согласно аналитическим данным в сфере информационной безопасности (далее-ИБ), в 2022 году число атак на российскую ИТ-инфраструктуру значительно увеличилось. Одними из главных объектов кибернападений являются государственные организации и промышленные предприятия, в том числе объекты КИИ.

На заседании круглого стола участники обсудили тему: «Обеспечение технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: создание отраслевых центров реагирования, производство и внедрение отечественных решений».

Участниками заседания рассмотрены вопросы: нормативного регулирования процесса обеспечения технологической независимости и безопасности КИИ, отраслевых элементов защиты от кибератак, особенностей организации и регулирования порядка перехода субъектов КИИ на использование отечественных решений, текущего статуса импортозамещения решений в сфере защиты, о роли отраслевых центров в повышении уровня обеспечения ИБ предприятий и отраслей в целом.

В дискуссии приняли участие представители Комитета Государственной Думы по информационной политике, информационным технологиям и связи, Министерства промышленности и торговли Российской Федерации, Министерства экономического развития Российской Федерации, Министерства внутренних дел Российской Федерации, Федеральной службы по техническому и экспортному контролю, компаний в области информационной безопасности, экспертных сообществ.

Представитель комитета Государственной Думы по информационной политике отметил, что законодательство о компьютерных преступлениях устарело и предложил модернизировать подходы и методологию принятия решений, приводя в пример

программу «Багбаунти», инициированную Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации. Участники круглого стола отметили, что деятельность специалистов по поиску уязвимостей, законодательно не закреплена и может рассматриваться, как незаконная деятельность, квалифицируемая ст. 272 УК РФ. В связи с этим, было выдвинуто предложение по определению нового вида деятельности по поиску уязвимостей в ПО за вознаграждение, а также предложение об определении границы ответственности специалистов по поиску уязвимостей на законных основаниях.

В своем докладе представитель Министерства экономического развития Российской Федерации отметил, что сроки перехода на полностью отечественные программные и аппаратные решения, для некоторых объектов КИИ нереалистичные, т.к. не учитывается специфика непрерывно действующих предприятий. В связи с этим, выдвинуто предложение рассмотреть возможность поэтапного перехода и проработать сейчас защиту уже существующего ПО и оборудования, до момента обеспечения предприятий нужным объемом надежных отечественных решений.

Обсуждая вопросы наличия оборудования, которое будет работать в рамках обеспечения безопасности КИИ, участники отметили дефицит отечественной аппаратной составляющей и проблемы с количеством необходимого оборудования, в связи с чем, было предложено увеличить меры поддержки производителей оборудования, имеющих серийное производство и якорных заказчиков. Кроме того, в целях сокращения времени на создание и апробацию таких решений, ООО «Уральским центром систем безопасности» было предложено создание технологических партнерств (научно-производственных объединений, консорциумов) по разработке, производству, техническому обслуживанию отечественной радиоэлектронной продукции и программно-аппаратных комплексов.

Представителем ОАО «РЖД» отмечены: активная работа внутреннего управляющего комитета по ИБ, а также внутриотраслевой обмен информацией в области ИБ с Министерством транспорта Российской Федерации. Однако, в целях оперативного взаимодействия и реагирования, требуется координация на межотраслевом уровне. В связи с чем участники предложили создать центр координации, который будет включать в себя представителей министерств и подведомственных служб, ключевых объектов КИИ, экспертного сообщества в области ИБ.

Представителем Федеральной службы по техническому и экспортному контролю была озвучена проблема, возникающая при проведении экспертизы проектов объекта КИИ, - экспертами не учитываются требования законодательства по мерам обеспечения защищенности объекта КИИ и зачастую они не находят отражения в проектной документации в виде закрепления проведения необходимых мероприятий. В этой связи, необходимо при проведении экспертизы проектной документации учитывать требования законодательства по обеспечению объектов КИИ средствами защиты необходимого уровня. Для чего требуется, чтобы специалисты в области экспертизы обладали профессиональными знаниями в области соблюдения норм по ИБ при проектировании объекта КИИ.

Учитывая изложенное и рассмотрев представленные на заседании материалы, секция «Обеспечение технологического суверенитета и информационной безопасности

Российской Федерации» Совета по развитию цифровой экономики при Совете Федерации Федерального Собрания Российской Федерации (далее – Секция)

решила:

1. Рекомендовать Министерству экономического развития Российской Федерации совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации рассмотреть возможность реализации поэтапного перехода объектов КИИ, имеющих специфику непрерывно действующих предприятий, на отечественные программные и аппаратные решения.

2. Рекомендовать Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации, Министерству финансов Российской Федерации, Министерству энергетики Российской Федерации, Министерству здравоохранения Российской Федерации, Министерству промышленности и торговли Российской Федерации, Министерству транспорта Российской Федерации, Федеральной службе по техническому и экспортному контролю рассмотреть целесообразность создания межотраслевого центра, который будет в себя включать представителей министерств и подведомственных служб, ключевых объектов КИИ, экспертного сообщества в области ИБ, в целях оперативного взаимодействия и реагирования на угрозы кибербезопасности.

3. Рекомендовать Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации активизировать работу по разработке законодательной инициативы, направленной на ввод в правовое поле деятельности по поиску уязвимостей в ПО за вознаграждение и определения границ ответственности специалистов по поиску уязвимостей.

4. Рекомендовать Министерству промышленности и торговли Российской Федерации:

4.1. в рамках механизмов финансирования обеспечить приоритетную поддержку проектов и технологических партнерств, вовлеченных в серийное производство оборудования, используемого для обеспечения безопасности КИИ;

4.2. рассмотреть возможность создания технологических партнерств (научно-производственных объединений, консорциумов) по разработке, производству, техническому обслуживанию отечественной радиоэлектронной продукции и программно-аппаратных комплексов.

5. Рекомендовать Министерству строительства и жилищно-коммунального хозяйства Российской Федерации совместно с Федеральным автономным учреждением «Главное управление государственной экспертизы» рассмотреть целесообразность:

5.1. внесения изменений в Градостроительный кодекс РФ и в Федеральный закон от 30.12.2009 N 384-ФЗ «Технический регламент о безопасности зданий и сооружений» в части исполнения требований по соблюдению законодательства по обеспечению объектов КИИ должным уровнем информационной безопасности;

5.2. создания образовательных программ повышения квалификации и семинаров по вопросам проведения государственной экспертизы проектной документации и

результатов инженерных изысканий, направленные на повышение уровня профессиональных знаний в области соблюдения норм по информационной безопасности при проектировании объекта КИИ.

6. Рекомендовать Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации и Банку России рассмотреть целесообразность разработки механизмов софинансирования затрат объектов КИИ в случаях, повлекших финансовые потери вследствие кибератак, а именно рассмотреть возможность создания Федерального закона, который вводит новые виды добровольного и обязательного страхования – страхование киберрисков.

7. Рекомендовать Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации и Министерству промышленности и торговли Российской Федерации рассмотреть целесообразность определения термина «доверенное оборудование» и требований к его использованию в различных отраслях.

8. Направить настоящее решение **Министерству экономического развития Российской Федерации**, **Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации, Министерству финансов Российской Федерации, Банку России, Министерству энергетики Российской Федерации, Министерству здравоохранения Российской Федерации, Министерству промышленности и торговли Российской Федерации, Министерству внутренних дел Российской Федерации, Министерству транспорта Российской Федерации, Министерству строительства и жилищно-коммунального хозяйства Российской Федерации, Федеральной службе по техническому и экспортному контролю,** участникам заседания секции.

Руководитель Секции «Обеспечение технологического суверенитета и информационной безопасности Российской Федерации» Совета по развитию цифровой экономики при Совете Федерации Федерального Собрания Российской Федерации
А.Г. Шейкин