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

16 марта 2023 года **г. Москва**

В условиях возросших киберугроз и уровня санкционного давления на Российскую Федерацию особое значение имеет формирование эффективных комплексных инструментов предупреждения и противодействия компьютерным атакам на информационные ресурсы объектов критической информационной инфраструктуры.

В состоявшейся дискуссии приняли участие представители Министерства цифрового развития, связи и коммуникаций Российской Федерации, Федеральной службы по техническому и экспортному контролю, Национального координационного центра по компьютерным инцидентам, Министерства промышленности и торговли Российской Федерации, а также члены рабочей группы по вопросам кибербезопасности Комитета Российского союза промышленников и предпринимателей по цифровой экономике.

Участниками были рассмотрены вопросы нормативного правового регулирования и практической реализации ключевых элементов обеспечения информационной безопасности объектов критической информационной инфраструктуры, безопасной разработки программного обеспечения,

дополнительных мер защиты персональных данных, методик и подходов к оценке уровня зрелости кибербезопасности предприятий.

В ходе обсуждения была отмечена важность комплексного подхода к обеспечению информационной безопасности и создание условий нормального функционирования объектов критической информационной инфраструктуры, а также предприятий отраслей в целом. Участники отметили стратегическое значение эффективной реализации требований, изложенных в Указах Президента Российской Федерации от 30 марта 2022 года № 166 и от 1 мая 2022 года № 250.

Заслушав и обсудив доклады и выступления, участниками было отмечено, что повышение уровня защищенности промышленных предприятий и отраслей, помимо формирования эффективных систем защиты информации, должно также базироваться на отраслевой специфике и выстроенной эффективной координации в области информационной безопасности. Производственные кооперации каждой отрасли обладают взаимосвязанной системой, отдельные элементы которой принадлежат различным компаниям и разнородны по своему программному и аппаратному наполнению, что, как следствие, порождает невозможность эффективного противостояния комплексным распределенным кибератакам, которые являются основным инструментарием кибергруппировок.

Кроме того, требуют проработки и реализации актуальные вопросы развития нормативной правовой базы, такие как: формирование института независимого аудита в сфере информационной безопасности, института добровольного страхования киберрисков, вопросы защиты значимых объектов критической инфраструктуры от угроз неправомерного использования беспилотных летательных аппаратов. Отдельно отмечен был вопрос острой кадровой потребности в специалистах и экспертах в области информационной безопасности.

Учитывая изложенное и рассмотрев представленные на заседании материалы представителей органов государственной власти и членов Рабочей группы по вопросам кибербезопасности Комитета Российского союза промышленников и предпринимателей по цифровой экономике, 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 цифрового развития, связи и коммуникаций Российской Федерации:**

1.1 Предусмотреть отдельную должность заместителя руководителя ответственного за информационную безопасность, который при этом не является руководителем цифровой трансформации органа.

1.2 При разработке законопроекта об ужесточении ответственности операторов персональных данных (далее – ПДн) за утечки ПДн, рассмотреть возможность введения, в качестве смягчающего обстоятельства, оценки соответствия операторов повышенным требованиям в сфере информационной безопасности, подтвержденной независимым аудитом, и использования добровольных механизмов минимизации ущерба субъектам персональных данных. А также изучить возможность исключения безвиновной ответственности операторов за утечку персональных данных.

2. **Рекомендовать Федеральной службе по техническому и экспортному контролю:**

2.1 Проработать вопрос формирования методик и подходов по инвентаризации ИТ активов компаний, в том числе в сегменте АСУ ТП.

2.2 Проработать вопрос нормативного правового закреплении компетенций отраслевых регуляторов, предусматривающих возможность формирования отраслевых компетенций и инструментов взаимодействия по вопросам информационной безопасности, позволяющих обеспечить координацию усилий и выработку инструментов по эффективному противодействию киберугрозам с учетом специфики отраслей. Рассмотреть возможность формирование методических рекомендаций в части определения специфики и функционала, реализуемого при отраслевом регулировании вопросов в области информационной безопасности.

2.3 Рассмотреть возможность формирования методики оценки уровня зрелости информационной безопасности в организациях с учетом необходимости определения фиксированного числа недопустимых событий и установления требований к срочности устранения уязвимостей. Проанализировать необходимость

нормативного правового закрепления обязательства организаций по регулярному (ежегодному) подтверждению уровня безопасности компаний с изменяющимися нормативными показателями.

3. **Рекомендовать Министерству транспорта Российской Федерации, Федеральному агентству воздушного транспорта Российской Федерации, при учете позиции Федеральной службы безопасности Российской Федерации**:

Изучить возможность предоставления правовых оснований и полномочий руководителям по обеспечению защиты воздушного пространства на объектах критической информационной инфраструктуры от беспилотных летательных аппаратов (далее – БПЛА), а также полномочий охранным предприятиям по использованию специальных средств борьбы с БПЛА, в том числе проектированию, монтажу и эксплуатационному обслуживанию технических средств противодействия БПЛА, включая лицензирование, с принятием соответствующих мер реагирования на их сигнальную информацию. В том числе, рассмотреть вопросы:

- Определения переченя организаций, для которых необходимы меры по обеспечению безопасности воздушного пространства;
- Внесения изменений требований по защите воздушного пространства в паспорта антитеррористической защищенности объектов;
- Введения экспериментального правового режима (ЭПР) в отношении тестирования технологий и нормативного регулирования обнаружения и противодействия нелегальным БПЛА;
- Разработки и организации программы профессионального обучения для работы со средствами противодействия БПЛА.

4. **Рекомендовать Министерству Финансов Российской Федерации, Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации, Центральному банку Российской Федерации:**

Организовать системную работу, при участии организаций в области информационной безопасности, по формированию унифицированных подходов и основ нормативного регулирования (базовых понятий и определений, а также методик) необходимых для осуществления добровольного страхования киберрисков предприятий.

5. **Направить настоящее решение в Министерство цифрового развития, связи и коммуникаций Российской Федерации, Федеральную службу по техническому и экспортному контролю, Федеральную службу безопасности Российской Федерации, Министерство финансов Российской Федерации.**

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