ОТП Отечественные Товаропроизводители

Торгово-промышленная палата Российской Федерации
В интересах бизнеса, во благо России

ЕАКЭ

АРСИБ

ПРОГРАММА МЕЖВЕДОМСТВЕННОЙ СЕССИИ:

«Безопасность критической информационной инфраструктуры (КИИ) предприятий и учреждений. Практика применения требований №187-ФЗ. Нововведения, порядок действий, риски и ответственность».

12-13 декабря 2019 года

© ООО Издательский дом "Отечественные Товаропроизводители" - 2019 | 101000, РФ, г. Москва, Чистопрудный бульвар, д.5, п.1, к.2 | ИНН 7707408799 | КПП 7707408799 | ОГРН 1187746181842 |+7 495 11 543 55 | www.otprod.ru | info@otprod.ru | office@otprod.ru

Модератор: Минин Виктор Владимирович, председатель Правления Ассоциации руководителей служб информационной безопасности (АРСИБ); член экспертного совета Евразийской ассоциации экспертов по защите киберпространства (ЕАК).

Экспертный состав:

Представитель ФСТЭК России;

Представитель Генеральной прокуратуры;

Представитель ФСБ России;

Представитель ФАС;

Акимов Кирилл Александрович, представитель НКЦКИ;

Бабин Игорь Николаевич, представитель страхового общества РЕСО-ГАРАНТИЯ;

Егорова Анна Георгиевна, начальник департамента сертификации ОПКиИТ – зам. руководителя органа по сертификации ВР/ОС Ассоциации по сертификации «Русский Регистр»;

Минаков Владимир Александрович, руководитель центра информационной безопасности «Icreate»;

Петренко Сергей Анатольевич, руководитель Центра информационной безопасности «Иннополис»;

Роенок Александр Анатольевич, директор по информационной безопасности «AST» (Advanced System Technologies);

Сафонов Валерий Васильевич, член Правления Евразийской ассоциации экспертов по защите киберпространства;

Харченко Андрей Викторович, директор проектов Центр кибербезопасности и защиты ПАО «Ростелеком»;

Лобанов Максим Иосифович, директор Учебного Центра Безопасности Информации «МАСКОН».

Представители российских компаний производителей средств защиты информации, предприятий субъектов КИИ.

12 ДЕКАБРЯ 2019 ГОДА

9.30-10.00	Сбор гостей. Утренний кофе.
10.00-13.00	**Обзор и практика применения законодательства в сфере Госсопка и безопасности КИИ.** – Презентация Ассоциации субъектов КИИ «КиберАльянс»; – Законодательное регулирование сферы по обеспечению безопасности автоматизированных систем управления производственными и технологическими процессами КИИ, а также системы государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России (ГосСОПКА). Разъяснение требований НПА, перспективы развития законодательства;

	– Мероприятия по выполнению требований №187-ФЗ; частые ошибки при подаче сведений; – Развертывание ведомственных сегментов ГосСОПКА; – Границы регулирования между ведомствами; – Рекомендации регуляторов.
13.00-14.00	Обеденный перерыв.
14.00-15.30	**Категорирование объектов КИИ. Разборка кейсов.** **Я – субъект КИИ. Что делать?** – Как и что отправить в ГосСОПКУ, если у меня ничего нет? – Я – коммерческое предприятие, зачем мне ТЗ и техпроект? – Схемы привлечения сторонних организаций на этом этапе («Техпроект под ключ», консультации). – Плюсы и минусы схем. – Перспективы привлечения к ответственности. Юридическая защита руководителей и специалистов служб информационной безопасности предприятий в случае возникновения уголовной и административной ответственности.
15.30-16.00	Кофе-брейк.
16.00-17.30	**Категорирование объектов КИИ. Разборка кейсов.** **Для тех, у кого есть выбор.** – Разница подходов к категорированию: плюсы и минусы самостоятельного категорирования, привлечения исполнителя для категорирования прямым договором или через торги. – Подводные камни самостоятельного категорирования: сколько выбрать объектов КИИ, как провести анализ критических бизнес-процессов и пр. **Для тех, у кого нет выбора.** – Как сыграть торги по 44-ФЗ и не проиграть. – Оценка надёжности поставщика.
17.30-18.00	Подведение итогов дня. Ответы на вопросы.

13 ДЕКАБРЯ 2019 ГОДА

09:30-10:00	Регистрация участников. Утренний кофе
10.00 – 10.45	**Категорирование объектов КИИ. Разборка кейсов.** – Анализ объектов КИИ; – Определение принадлежности хотя бы одного из объектов к сферам КИИ. – Определение видов деятельности предприятия (управленческих, технологических, производственных, финансово-экономических), видов субъектов; – Выявление критических процессов; – Определение объектов КИИ, обрабатывающих информацию, определение критических процессов; – Формирование перечня объектов КИИ, подлежащих категорированию; – Присвоение категорий значимости; – Отправка сведений в ФСТЭК России.
10.45-11.30	**Установление требований к обеспечению безопасности ЗО КИИ. Составление модели угроз. Разработка технического проекта.** – Порядок оценки полноты и достаточности существующих организационных и технических мер по обеспечению безопасности ЗО КИИ; – Разработка технического задания на создание подсистемы безопасности;

	– Анализ угроз безопасности информации и разработка модели угроз безопасности информации; – Порядок проектирования подсистемы безопасности ЗО КИИ; – Порядок разработки рабочей (эксплуатационной) документации на значимый объект.
11.30-12.00	Кофе-брейк.
12.00-13.00	**Внедрение организационных и технических мер по обеспечению безопасности ЗО КИИ и ввод его в действие.** – Порядок выбора, установки и настройки средств защиты информации; – Порядок разработки организационно-распорядительных документов; – Порядок внедрения организационно-распорядительных мер по обеспечению безопасности ЗО КИИ, испытания, опытная эксплуатация; – Порядок анализа уязвимости ЗО КИИ и принятие мер по их устранению, приемочные испытания ЗО КИИ.
13.00-14.00	Обеденный перерыв.
14.00-16.30	**Внедрение организационных и технических мер по обеспечению безопасности ЗО КИИ и ввод его в действие. Разбор кейсов.** **Выбор и внедрение технических средств обеспечения безопасности объектов КИИ:** – Выбор огромен или его нет? – Отечественные vs импортные средства защиты. – «Запатчить всё!» или «Нет средства – не будет глючить». **Секция 1: Защита ИС:** – Собственные средства защиты vs услуги мониторинга. – «Запретить всё, что небезопасно» или «Всё в угоду бизнесу». – Встроенные vs наложенные средства защиты. – Добавить ещё один уровень защиты или запатчить ещё дыр в системе. **Секция 2: Защита ИТКС** – Эшелонированная защита или минимум задержек? – Средства защиты сети: «всё в одном» или «не класть все яйца в одну корзину»? – Зачем нужна 5-летняя техподдержка? – Если остался бюджет, то, как усилить защиту: шифрование vs New Generation. **Секция 3: Защита АСУ ТП.** – Построение системы защиты: «не трогай» или «не навреди». – Канал связи с иностранной техподдержкой: риски и возможности. – Меры безопасности: технические или организационные. – Продажа риска провайдеру услуг: границы применимости. **Секция 4: Защита сетей связи** – Я не провайдер услуг связи и подключён к ГосСОПКа. Мне всё равно и это надо? – Российские сети связи: отказоустойчивость, скорость передачи и ГОСТовское шифрование. – Где найти реестр поставщиков услуг.
16.30-17.00	Подведение итогов дня. Ответы на вопросы.

РЕГИСТРАЦИЯ:

- **на сайте:** otprod.ru
- **по телефонам:** 8 (495) 115-43-55
- **по e-mail:** info@otprod.ru, abramov@otprod.ru
- **контактное лицо:** Абрамов Андрей Александрович