---

5 февраля 2025

08:30 - 18:00

РЕГИСТРАЦИЯ УЧАСТНИКОВ И ОТКРЫТИЕ ПРОФЕССИОНАЛЬНОЙ ВЫСТАВКИ «ЭКОНОМИКА ДАННЫХ И КИБЕРБЕЗОПАСНОСТЬ»
НОВЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ГОСУДАРСТВА, ЭКОНОМИКИ И ГРАЖДАН

10:00 - 12:00

БОЛЬШОЙ НАЦИОНАЛЬНЫЙ ФОРУМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «ИНФОФОРУМ-2025» - ПЛЕНАРНОЕ ЗАСЕДАНИЕ
ТЕХНОЛОГИЧЕСКОЕ ЛИДЕРСТВО И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ В ИНФОРМАЦИОННОЙ СФЕРЕ ДО 2030 ГОДА

Вопросы для рассмотрения:

1. Национальные цели развития Российской Федерации в соответствие с Указом Президента Российской Федерации от 7 мая 2004 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» и центральные задачи в сфере обеспечения информационной безопасности граждан, организаций и государства.
2. Фактическое состояние уровня обеспечения информационной безопасности Российской Федерации с точки зрения государственных регуляторов, руководителей министерств и ведомств, регионов Российской Федерации, представителей крупных корпораций, специалистов. Что важно сделать в ближайшее время.
3. Вопросы международной информационной безопасности. Мнения друзей и партнеров.
4. Цифровые технологии развиваются постоянно, новые вопросы вносит переход на отечественные ПО и ПАК. Отрасль информационной безопасности догоняет, опережает или предугадывает новые риски. Тренды сегодняшнего дня.
5. Темы, вынесенные в отдельные дискуссии на Инфофоруме или те, о которых всё равно пора говорить.

12:00 - 12:15

«СЕРЕБРЯНЫЙ КИНЖАЛ» - XXII ЦЕРЕМОНИЯ НАГРАЖДЕНИЯ ЛАУРЕАТОВ
ПРОФЕССИОНАЛЬНАЯ ПРЕМИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Профессиональная премия учреждена Оргкомитетом Национального форума информационной безопасности «Инфофорум» в 2004 г. и является символом признания профессионального вклада специалистов и организаций в развитие и становление безопасного информационного общества в Российской Федерации.
«Серебряный кинжал» присуждается за личный вклад в укрепление системы информационной безопасности в Российской Федерации, за реализованные проекты по созданию систем информационной безопасности в области промышленности, энергетики, транспорта, кредитно-финансовой сферы, государственного управления, управления вооруженными силами, оказания электронных услуг, регионального управления, за укрепление международного профессионального сотрудничества. Престиж премии подчеркивают имена ее обладателей. За эти годы лауреатами премии стали более 150 специалистов и коллективов из России и зарубежных стран.

Список награжденных за 2004-2024 гг.

Номинации 2025 года

Победителей в конкурсе Национальной премии определяет Экспертный совет Национального форума информационной безопасности Инфофорум. Председатель Совета - **Шойтов Александр Михайлович**, заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации, президент Академии криптографии Российской Федерации.

13:00 - 14:30

КИБЕРИНЦИДЕНТЫ-2024/25. ТЕНДЕНЦИИ СОВРЕМЕННЫХ УГРОЗ И ПЕРЕДОВЫЕ МЕТОДЫ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ
ТЕМАТИЧЕСКАЯ СЕССИЯ 1.

Вопросы для рассмотрения:

1. Статистика киберинцидентов, география и отраслевая специфика организаций, находящихся в эпицентре киберугроз.
2. Актуальные тактики, техники и новые инструменты киберпреступников.
3. Особенности киберрисков в зависимости от отраслевой принадлежности: государственные организации, финансовый сектор, промышленные предприятия, транспортные организации, предприятия розничной торговли, предприятия телеком отрасли и ИТ-компании, медицинские учреждения, образовательные учреждения, СМИ.
4. Передовые методы и средства защиты для повышения уровня защищенности организаций и граждан, ликвидации последствий кибератак.
5. Практика взаимодействия государственных регуляторов, SOC-центров и крупных отраслевых компаний.

13:00 - 14:30

ВОПРОСЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЭКОНОМИКА ДАННЫХ И ОБЕСПЕЧЕНИЕ ДОВЕРИЯ НА МЕЖДУНАРОДНОМ УРОВНЕ
ТЕМАТИЧЕСКАЯ СЕССИЯ 2.

Вопросы для рассмотрения:

1. Российские инициативы в сфере международной информационной безопасности.
2. Страны ОДКБ: сотрудничество в сфере борьбы с киберпреступностью. Новые направления, требующие внимания дружественных стран.
3. Сотрудничество в рамках ШОС: противодействие использованию сети Интернет в террористических, сепаратистских и экстремистских целях.
4. Опыт дружественных стран по реагированию на современные вызовы и угрозы информационной безопасности.
5. Экспортный потенциал отрасли информационной безопасности в рамках сотрудничества стран ЕАЭС, ШОС, БРИКС, СНГ, ОДКБ. Успешные практики.
6. Международное сотрудничество по усилению правовой базы борьбы с преступностью в сфере ИТ и цифровой экономики. Сотрудничество органов прокуратуры и следствия, негосударственных организаций в сфере противодействия информационной преступности.

13:00 - 16:15

ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ: НОВЫЕ ЗАДАЧИ И РЕШЕНИЯ
ТЕМАТИЧЕСКАЯ СЕССИЯ 3.

Сессия проводится с перерывом на кофе-брейк.

Вопросы для рассмотрения:

1. С 1 января 2025 г. объекты критической инфраструктуры должны перейти на отечественные решения для обеспечения информационной безопасности (в соответствии с Указом Президента России №250). Состояние и задачи обеспечения безопасности информационного пространства Российской Федерации в современных условиях.
2. Кибербезопасность в промышленности и ТЭК.
3. Инфобезопасность медицинской инфраструктуры.
4. Вопросы сетевой безопасности объектов КИИ.
5. Выстроить приоритеты в системе информационной безопасности объектов КИИ. Вопросы категорирования объектов КИИ: требования и типовые недостатки.
6. Комплексные решения для обнаружения и предотвращения компьютерных атак на информационные ресурсы, защиты от угроз терроризма, экстремизма и внешнего информационного вторжения на АСУ ТП.
7. Защита от внутренних угроз как обязательный элемент защиты КИИ.
8. Отраслевые особенности центров мониторинга информационной безопасности. Опыт построения коммерческого SOC: вопросы проблемы, решения.

14:45 - 16:15

БЕЗОПАСНОСТЬ КОММУНИКАЦИЙ В ЭПОХУ КВАНТОВЫХ ТЕХНОЛОГИЙ
ТЕМАТИЧЕСКАЯ СЕССИЯ 4.

Вопросы для рассмотрения:

1. Квантовые технологии, квантовые коммуникации и постквантовая криптография в России и мире: состояние, успехи, направления.
2. Перспективы использования квантовых технологий в финансовой сфере. Криптоэкономика и кибербезопасность.
3. Что такое квантовый блокчейн.
4. Квантовые магистральные сети. Как в РЖД работают над технологиями будущего. Развитие на территории России единого мультимодального транспортно-логистического пространства на основе отечественных цифровых технологий.
5. Недостатки и уязвимости квантовых коммуникаций.
6. Интернет вещей и квантовая защита.
7. Передовые методы защиты информации, сохранения конфиденциальности и предотвращения утечки данных при их обработке в распределенных средах.

14:45 - 16:15

NGFW
ТЕМАТИЧЕСКАЯ СЕССИЯ 5.

Готовится совместно с компанией Айдеко

NGFW – комплексная защита корпоративной сети от сетевых атак и вредоносного ПО. Мифы и реальность российского рынка NGFW. Критерии сравнения, анализ. Приоритеты российских производителей. Что предложат российские производители в 2025 году.

16:30 - 18:00

ДОВЕРЕННЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ
ТЕМАТИЧЕСКАЯ СЕССИЯ 6.

Вопросы для рассмотрения:

1. Новые возможности для развития деятельности организаций и граждан, риски использования ИИ в условиях экономики данных. ИИ уже работает – расскажите как.
2. Кооперация государства, науки и бизнеса для обеспечения интеграции доверенного ИИ в повседневную жизнь так, чтобы достичь эффективности и потом не жалеть.
3. Методы и решения для обеспечения доверия и защищённости технологии ИИ с использованием криптографии.
4. Защищённые технологии для работы с различными типами данных, включая обезличенные персональные данные, с использованием технологий машинного обучения и методов ИИ.
5. Отечественные программные продукты и программно-аппаратные комплексы (ПАК),

использующих технологии доверенного и защищённого искусственного интеллекта.
6. Как повысить квалификацию специалистов по разработке отечественных программных продуктов и ПАК с применением технологий доверенного и защищённого ИИ. Опыт ведущих вузов и центров подготовки профессиональных кадров.
7. Проекты разработки и тестирования технологий доверенного и защищённого ИИ. Направления научных исследований с использованием ИИ.

16:30 - 18:00

ИМПОРТОНЕЗАВИСИМОСТЬ ИТ-ОТРАСЛИ И ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ
ТЕМАТИЧЕСКАЯ СЕССИЯ 7.

Вопросы для рассмотрения:

1. Цифровая трансформация и импортозамещение в отраслях экономики Российской Федерации. Оценка темпов перехода на использование отечественных решений, итоги закупок 2024 года, оценка действия правительственных директив, текущие задачи.
2. Существующие недостатки в реализации программ импортозамещения.
3. Отечественные ПАКи для государства и бизнеса. Проблемы и успешные практики внедрения. Приоритетные направления развития отечественной радиоэлектроники.
4. Цифровые инструменты финансирования. Факторинг в сфере комплексных решений и АПК для защиты информации. Инструменты государственной и банковской поддержки закупок предприятий-заказчиков отечественных сертифицированных программных продуктов.
5. Тенденции развития отечественной отрасли ИБ и особенности цифровой трансформации в крупных корпорациях. Скорость и качество решений.
6. Защита информации от внутренних угроз в условиях обеспечения технологического суверенитета.
7. Экосистемы как стратегия импортозамещения и перехода на российские ИТ-решения.

16:30 - 18:00

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ (ЦОДЫ) И ОБЛАЧНЫЕ РЕШЕНИЯ. СОХРАНЕНИЕ И ЗАЩИЩЕННОЕ ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ
ТЕМАТИЧЕСКАЯ СЕССИЯ 8.

Вопросы для рассмотрения:

1. Цифровая память, сохранение информационного наследия – уже не только общественно-значимая задача и вопрос отдельных организаций. Это предмет геополитического противоборства. Сколько крупных ЦОДов действует в России и что создано в последнее время?
2. Цифровое хранилище. Корпоративные и государственные ЦОДы. Вопросы кибербезопасности, устойчивости и отказоустойчивости.
3. Вопросы выбора приоритетов хранения при постоянно возрастающих объемах информации в цифровом мире.
4. Российские облачные сервисы для хранения данных. Преимущества и недостатки основных серверов («Яндекс.Диск»; «Облако Mail.ru»; «СберДиск»; «Вторая память» МТС; «Облако Билайн»; VK Cloud; Selectel; Ростелеком и др.). Решения для обеспечения

кибербезопасности.
5. Является ли облачный провайдер субъектом КИИ.
6. Обеспечение цифрового доступа к информации и конфиденциальности информации, хранящейся в цифровом архиве.
7. Вопросы объединения и обмена информацией между цифровыми архивами. Как обеспечить информационную безопасность данных.
8. Дата-центры: использование ИИ и нейросетей при анализе больших данных для государства, региона, организаций. Возможности и риски, которые нужно преодолеть. Есть ли квалифицированный заказчик такой информации и порядок ее использования?

17:45 - 20:00

ДЕЛОВОЙ ВЕЧЕРНИЙ ФУРШЕТ ИНФОФОРУМА
МЕСТО, ГДЕ СТАНОВЯТСЯ ДРУЗЬЯМИ

---

6 февраля 2025

09:00 - 10:00

ДЕЛОВОЙ ЗАВТРАК В ФОРМЕ ДИСКУССИОННОГО КЛУБА ИНФОФОРУМА-2025
РОССИЙСКИЕ РЕГИОНЫ: ЦЕНТРАЛЬНЫЕ ПРОБЛЕМЫ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕГОДНЯ.

Приглашаются руководители министерств, департаментов и управлений субъектов Российской Федерации. К участию также приглашены представители регуляторов отрасли информационной безопасности, ведущих федеральных министерств и ведомств. Представители предприятий – по согласованию с Оргкомитетом.
Заседание проходит без участия прессы и без трансляции в сети интернет.

10:00 - 11:30

ЭЛЕКТРОННАЯ ТОРГОВЛЯ И ФИНАНСОВЫЕ УСЛУГИ: ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ
ТЕМАТИЧЕСКАЯ СЕССИЯ 9.

Вопросы для рассмотрения:

1. Роль данных в электронной торговле и цифровой экономике. Динамика развития рисков и угроз ИБ в финансовой сфере.
2. Цифровой рубль, цифровые платежи и цифровые трансграничные транзакции. Направление развития и вопросы кибербезопасности.
3. Помогут ли цифровые финансовые активы (ЦФА) и криптовалюта в условиях экономических санкций. Подводные камни и необходимые правовые решения.
4. «БРИКС Пэй — БРИКС Бридж» - платформа для трансграничных платежей. Решения для повышения устойчивости и независимости расчетов в условиях текущей геополитической

ситуации.
5. Где уже успешно применяются ЦФА и блокчейн-технологии в условиях экономики данных. Вопросы защита информации.
6. Цифровая валюта и блокчейн-технологии в объективе преступной деятельности.
7. Роль методов криптографии и систем анализа социальных сетей для расследования преступлений в данной сфере.
8. Трансграничные платежные системы и технологии ИИ. Необходимость умных решений.

10:00 - 11:30

РОССИЙСКИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ О БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ СОБЫТИЯМИ БЕЗОПАСНОСТИ
ТЕМАТИЧЕСКАЯ СЕССИЯ 10.

Вопросы для рассмотрения:

1. Современные SIEM-системы – системы сбора, мониторинга и анализа событий безопасности в режиме реального времени. Лидирующие российские решения.
2. Опыт использования современных ситуационных центров и SOC в центре и на местах. Анализ угроз в кризисных ситуациях в госуправлении и деятельности объектов критической информационной инфраструктуры.
3. Технологии IRM (управление правами на информацию) – системы защиты конфиденциальной информации от несанкционированного доступа. Преимущества и проблемы, связанные с IRM. Актуальность грамотной внутренней защиты.
4. Вопросы создания и совершенствования экспертных баз для сокращения скорости реакции на информацию о конкретных внутренних и внешних угрозах безопасности.
5. Задача создания отраслевых центров мониторинга в сфере информационной безопасности в современных условиях.

11:45 - 13:15

КИБЕРБЕЗОПАСНОСТЬ РОЗНИЧНОЙ ТОРГОВЛИ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ
ТЕМАТИЧЕСКАЯ СЕССИЯ 11.

Вопросы для рассмотрения:

1. Возможные кибератаки и угрозы информационной безопасности в ритейле: кража данных, DDoS-атаки, нарушение цепочек поставок, остановка продаж, недоступность сайта, мошенничество в интернет-магазине и др.
2. Новые требования законодательства (Федеральный закон от 8 августа 2024 г. № 233-ФЗ вступит в силу с 01.09.2025) и усиление контроля за утечками персональных данных. Новые обязанности документооборота для юридических лиц.
3. Как реагирует на эти требования российский рынок информационной безопасности. Современные средства для технической защиты персональных данных.
4. Оценка уровня защищенности российской системы розничной торговли.

11:45 - 13:15

КАДРЫ НАСТОЯЩЕГО И БУДУЩЕГО. ПОТРЕБНОСТИ ПРАКТИКИ
ТЕМАТИЧЕСКАЯ СЕССИЯ 12.

Вопросы для рассмотрения:

1. Острая необходимость в квалифицированных кадрах в сфере ИБ в органах власти и на предприятиях основных отраслей экономики России. Состояние и тенденции в решении проблемы.
2. Цифровая зрелость» ключевых отраслей экономики, социальной сферы и государственного управления. Оценка рисков и угроз информационной безопасности. Есть ли отрасли, где «кадры нужны любые, но сейчас». Что это даст.
3. Что могут и предлагают российские вузы, центры дополнительного образования и корпоративные школы в условиях тотальное импортозамещение ПО и аппаратных решений для государства, промышленности и бизнеса. Проблемы и успешные кейсы.
4. Вопросы интеграции ведущих ИТ-компаний и профильных вузов. Организационные меры. Нужно создавать научные советы с участием сертифицированных преподавателей-практиков.

13:30 - 15:00

ДИПФЕЙКИ, АККАУНТЫ-ДВОЙНИКИ, ПОДМЕНА КОНТЕНТА И ДР. КАК УПРАВЛЯТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СМИ
ТЕМАТИЧЕСКАЯ СЕССИЯ 13.

Вопросы для обсуждения:

1. СМИ и телевидение в цифровом мире. Защита информации и вопросы киберпротивостояния.
2. Фейковая информация: технологические решения для противодействия и укрепления информационного суверенитета.
3. Защита от подмены информации в контенте отечественных СМИ и телевидения.
4. Дипфейки и искусственный интеллект в Интернете и средствах массовых коммуникаций. Технические средства определения фейков. Возможность создания продуктов для массового гражданского использования.
5. Сетевая безопасность в политике информационной безопасности интернет-СМИ и телевидения.
6. Информационная безопасность в сфере культуры и образования в условиях информационного противоборства.
7. Вопросы развития правового регулирования для предотвращения деструктивного информационно-технологического воздействия на информационные ресурсы Российской Федерации и дружественных стран.
8. Есть ли опыт создания профессиональных центров информационного противоборства и центров обучения специалистов в условиях информационной войны. Необходимость государственной поддержки.