https://ru-bezh.ru/otchyotyi-o-sobyitiyax/64540-infoforum-2026-dostup-k-gossektoru-podtverzhden-indeks-43

«Инфофорум-2026», прошедший 28–29 января в московском кластере «Ломоносов», собрал свыше 2000 очных и 1000 онлайн-участников, представителей федеральных министерств, ведомств и ключевых ИТ-компаний. Топ-менеджеры ведущих отечественных вендоров обсудили ход импортозамещения в сфере критически важных ИБ-решений, защиту объектов КИИ, реализацию второго антифрод-пакета и многое другое. Журнал RUБЕЖ оценил мероприятие по 13 критериям в рамках авторской методики Индекса отраслевых мероприятий. Итоговый показатель — 4,3 балла из 5.

Текст: Биктимир Абдрашитов, Дмитрий Воронин

_____

Методика оценки мероприятия в рамках Индекса мероприятий журнала RUБЕЖ

Индекс учитывает 13 критериев, среди которых периодичность проведения, площадь выставки, уникальность экспозиции и другие значимые параметры. По каждому критерию выставляется оценка от 1 до 5 баллов по следующей шкале:

5 баллов — превосходный, эталонный уровень;

4 балла — выше среднего, с выраженными преимуществами;

3 балла — средний, удовлетворительный уровень;

2 балла — ниже среднего, требует улучшения;

1 балл — неудовлетворительно.

Итоговый индекс мероприятия рассчитывается как среднее арифметическое всех 13 оценок.

_____

1. Периодичность и регулярность: 5/5

«Инфофорум» — первое и старейшее специализированное мероприятие в сфере информационной безопасности в России. Мероприятие проходит ежегодно с 2001 года под кураторством Ассоциации «Национальный форум информационной безопасности “Инфофорум”», учрежденной по инициативе Аппарата Совета Безопасности Российской Федерации и Комитета Государственной Думы по безопасности.

Форум позиционируется как некоммерческая, общественно-государственная площадка для выработки консенсуса между регуляторами, бизнесом, наукой и экспертным сообществом по ключевым вопросам обеспечения информационной безопасности страны.

Главная цель «Инфофорума» — формирование стратегических рекомендаций для органов власти,

согласование нормативно-правовой базы, обсуждение приоритетов защиты КИИ, импортозамещения, кадровой политики и международной ИБ. Это подчеркивается самим форматом:

- пленарное заседание в 2026 году открыли представители Совета Безопасности РФ (Дмитрий Грибков), Госдумы (Сергей Боярский), Минцифры (Александр Шойтов), ФСТЭК (Елена Торбенко).
- в рамках форума ранее заключались меморандумы о сотрудничестве между Ассоциацией «Инфофорум» и региональными министерствами (например, Тюменской области в 2025 г., Перми и Красноярска в 2024 г.) — прямое свидетельство того, что форум воспринимается как инструмент реализации госполитики на местах.

2. Посещаемость: 4/5

В 2026 году Форум [собрал](https://infoforum.ru/uchastniki-infoforuma-2026) около 2000 очных участников и свыше 1000 онлайн-зрителей. Аудитория была представлена специалистами, топ-менеджерами ИБ-отрасли, чиновниками, включая зарубежных гостей из Беларуси и Казахстана. В 2025 году организаторы также фиксировали количество участников на уровне 3000 специалистов.

3. С**татус спикеров: 5/5**

Пленарное заседание «Инфофорума-2026» открыл Александр Шойтов, заместитель Министра цифрового развития, связи и массовых коммуникаций РФ и президент Академии криптографии РФ. Под его модерацией прошла дискуссия на тему «Приоритеты информационной безопасности России: чтобы быть на шаг впереди», в которой ключевые регуляторы страны обозначили стратегические направления на 2026–2027 годы.

Тематические сессии форума прошли в трех залах («Молекула», «Физика» и «Атом») и были посвящены актуальным вызовам — защите КИИ, импортозамещению, ИИ в кибербезопасности, международному сотрудничеству и квантовым технологиям.

Ниже — ключевые спикеры с должностями и темами их выступлений.

Федеральные регуляторы и органы власти

- [Грибков Дмитрий Геннадьевич](https://ru-bezh.ru/meropriyatiya/news/26/01/28/v-moskve-startoval-infoforum-2026-ozvucheny-prioritety-informats)- [Боярский Сергей Михайлович](https://ru-bezh.ru/meropriyatiya/news/26/01/28/sergey-boyarskiy-na-infoforume-2026-pervyy-antifrod-paket-snizil) — депутат Государственной Думы, председатель Комитета Государственной Думы по информационной политике, информационным технологиям и связи; доклад о первом и втором антифрод-пакетах;
- Торбенко Елена Борисовна —начальник Управления Федеральной службы по техническому и экспортному контролю (ФСТЭК России); доклад «Изменения законодательства по обеспечению безопасности критической информационной инфраструктуры. Общие проблемы реализации требований законодательства»;
- Иванов Алексей Владимирович — заместитель директора Национального координационного центра по компьютерным инцидентам (ГосСОПКА); доклад «О совершенствовании правового и организационного обеспечения функционирования ГосСОПКА»;
- Дождев Владимир Святославович — директор Департамента цифровых технологий

Министерства промышленности и торговли Российской Федерации; доклад «Об эксперименте по повышению эффективности противодействия кибератакам на объекты КИИ отраслей промышленности за счет интеллектуальной автоматизации»;

- Букин Дмитрий Васильевич — заместитель директора Департамента международной информационной безопасности МИД России; доклад «Актуальные вопросы международной информационной безопасности на внешнем контуре»;

- Уваров Вадим Александрович — директор Департамента информационной безопасности Банка России; доклад «Актуальные вопросы обеспечения информационной безопасности кредитно-финансовой сферы»;

- Сергиенко Сергей Владимирович —директор Департамента развития искусственного интеллекта и больших данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации; доклад в рамках сессии «Искусственный интеллект и информационная безопасность»;

- Хасин Евгений Владимирович — врио директора Департамента обеспечения кибербезопасности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации; модерация сессий по доверенным ПАКам.

Региональные представители

- Логинов Станислав Игоревич — заместитель губернатора, директор Департамента информатизации Тюменской области; доклад «Российские регионы: центральные проблемы и насущные задачи в сфере информационной безопасности. Опыт Тюменской области»;

- Ципорин Павел Игоревич — заместитель губернатора, директор Департамента информационных технологий и цифрового развития Ханты-Мансийского автономного округа — Югры; модератор сессии «Умный и Безопасный город в современных условиях».

Международное участие и межгосударственные структуры

- Неверовский Александр Викторович — заместитель Государственного секретаря Совета Безопасности Республики Беларусь; доклад «Обеспечение информационной безопасности Союзного Государства в современных условиях»;

- Семериков Валерий Анатольевич — заместитель Генерального секретаря ОДКБ;

- Шамбулов Улыкбек Кадыржанович — первый заместитель Председателя Правления АО «Государственная техническая служба», руководитель НКЦИБ Республики Казахстан; доклад «О некоторых аспектах реагирования на современные вызовы и угрозы обеспечения информационной безопасности».

Отраслевые лидеры и институты развития

- Мирошников Борис Николаевич — президент Национальной ассоциации международной информационной безопасности, сопредседатель Оргкомитета Инфофорума, вице-президент ГК «Гарда»; модерация и выступление в сессии «Международная информационная безопасность: центральные проблемы и решения»;

- Гореславский Алексей Сергеевич — директор АНО «Институт развития интернета», председатель Общественного совета при Минцифры России; участие в сессии «Медиапространство и проблемы информационной безопасности»;

- Качалин Игорь Федорович — генеральный директор АНО «Национальный технологический центр цифровой криптографии», член Оргкомитета Инфофорума; модерация сессии «Искусственный интеллект и информационная безопасность»;

- Калашников Артем Игоревич — управляющий директор Центра информационной безопасности

дочерних и зависимых обществ, Банк ГПБ (АО); выступление в сессии «Искусственный интеллект и информационная безопасность» и модерация сессии «Квант и пост-квант»;

- Маслов Владимир Андреевич — директор Департамента цифровых технологий ТПП России, член Оргкомитета Инфофорума; модерация сессии «Импортонезависимость и информационная безопасность: актуальные вопросы в сфере энергетики, промышленности, транспорта».

4. Эк**спозиция и новинки: 5/5**

Экспозиция «Инфофорума-2026» была выстроена как [демонстрация уже внедренных решений](https://ru-bezh.ru/meropriyatiya/news/26/01/29/rossiyskie-kompanii-predstavili-resheniya-dlya-importozameshchen). Программные продукты прошли все этапы государственной сертификации для развертывания в условиях повышенных требований ФСТЭК и ФСБ. Среди них системы мониторинга угроз, платформы управления событиями безопасности, решения для построения доверенных ИТ-инфраструктур на базе Linux, а также аппаратные платформы для размещения средств защиты информации.

Вот некоторые из представленных продуктов:

- NGFW Novum от компании Ideco (NGFW, или Next-Generation Firewall — «межсетевой экран нового поколения», прим. ред.) — это enterprise-решение нового поколения, построенное на современной архитектуре DPDK+VPP, обеспечивает высокую и предсказуемую производительность даже при включении всех функций безопасности;

- СКЗИ «Застава 8» от «Элвис-Плюс» — завершенный в 2024 году импортозамещенный комплекс криптографической защиты на базе доработанной open-source операционной системы с усиленной безопасностью для объектов КИИ и в сегменте АСУ ТП;

- аппаратные платформы от компании «Новые платформы» на базе процессоров Intel Xeon 4 и 5 поколений, предназначенные для создания межсетевых экранов нового поколения NGFW, криптошлюзов и других сетевых устройств.

5. Лидеры рынка: 5/5

Участники «Инфофорума-2026» представили решения, подтверждающие готовность российского ИБ-рынка выполнять требования регуляторов и защиты КИИ в условиях технологического суверенитета.

СберТех впервые публично представил свою систему AI Security Gateway — шлюз безопасности для генеративного ИИ. Компания также анонсировала услугу AI Red Team — имитацию атак APT-групп на ИИ-инфраструктуру для выявления уязвимостей до запуска в эксплуатацию.

РТК-ЦОД (дочерняя структура «Ростелекома») представил практику размещения объектов КИИ в доверенных облачных средах. Заместитель директора по ИБ Иван Синецкий рассказал, как заказчики могут использовать сертифицированные облака для соблюдения требований №187-ФЗ без потери контроля над данными и процессами.

АО «Аладдин Р.Д.» представило комплексную стратегию построения доверенной ИТ-инфраструктуры на базе Linux. Генеральный директор Сергей Груздев продемонстрировал, как с помощью отечественных решений — Aladdin Enterprise CA, SecurLogon и аппаратных токенов JaCarta — можно реализовать корпоративную PKI-инфраструктуру, аналогичную Microsoft Active Directory, и выполнить требования 117-го приказа ФСТЭК. Это особенно актуально для организаций, которые переходят с Windows на российские ОС и сталкиваются с отсутствием встроенных механизмов доверенной аутентификации.

ГК «Гарда» сфокусировалась на защите от внутренних угроз — обязательном элементе для объектов КИИ первой категории. Директор по развитию бизнеса Денис Батранков продемонстрировал, как решения Garda NDR, Garda DLP и Garda DBF позволяют выявлять аномалии в поведении пользователей, контролировать передачу данных через разрешенные каналы и предотвращать саботаж со стороны сотрудников с легитимным доступом.

UserGateпредставил результаты одного из крупнейших проектов импортозамещения в России — замену Check Point 64000 в ЦОДе крупной добывающей компании. Менеджер по развитию Кирилл Прямов сообщил, что решение UserGate DCFW обеспечивает производительность до 880 Гбит/с на L4-трафике и успешно обрабатывает 130 000 правил межсетевого экрана.

«Код Безопасности» принял участие в экспертной дискуссии «Не все NGFW одинаковые», где руководитель отдела продвижения продуктов Павел Коростелев обсудил вопросы технологической зрелости российских межсетевых экранов, их интеграции с SIEM/SOAR и готовности к работе в высоконагруженных сетях.

Также на форуме были представители АО «ИнфоТеКС», «Элвис-Плюс», «Новые платформы», Ideco, SECURITM, «Базальт СПО», Xello, ООО «АйТи БАСТИОН», NGENIX, «Р7-ОФИС», ООО «Клауд Атлас», ГК «Конфидент», SolidLab, CodeScoring, iTPROTECT, ООО «ПК ТС», компании «Мультифактор», ГК ЦРТ, ООО «ИЦСБ», «А2 Клауд», UDV Group, «Альтиус Лаб», «МТС ID для бизнеса», «Кибердом» и другие.

6. Площадь выставки и масштабы стендов: 3/5

Экспозиция на двух этажах заняла более 20 стендов среднего формата в кластере «Ломоносов». Для ИБ-отрасли, где продукты преимущественно программные, это объяснимо: физическая демонстрация решений ограничена. Каких-то стилизованных или креативных стендов замечено не было. Солидная часть просторных залов на обоих этажах пустовала. Пройтись по всей площади выставки, даже вглядываясь в информацию на стендах, заняло от силы 10 минут.

7. Статус представителей компаний на стендах: 4/5

Компании на стендах представляли преимущественно продакт-менеджеры и маркетологи (по 23 человека на стенд). Однако на ключевых стендах присутствовали генеральные и технические директоры (, директор департамента специальных работ в «Элвис-Плюс» Егор Комаров, технический директор Ideco Марк Коренберг) и основатели компаний (Сергей Груздев, компания «Алладин»).

8. Деловая программа: 5/5

Деловая программа «Инфофорума-2026» состояла из 12 тематических сессий, более 80 выступлений и была выстроена вокруг практической реализации требований регуляторов, а не декларативных дискуссий.

На пленарном заседании Сергей Боярский (председатель ИТ-комитета Госдумы) представил итоги первого антифрод-пакета: снижение мошенничества на 25% в 2025 году. Он анонсировал второй пакет, направленный на борьбу с дипфейками и автоматизированными мошенническими схемами, с запуском «тревожной кнопки» в мобильном приложении платформы противодействия

кибермошенничеству. Его промышленная эксплуатация запланирована на 2026 год.

Дмитрий Грибков, помощник Секретаря Совета Безопасности РФ, сообщил, что аппаратом Совбеза разрабатывается новая редакция Доктрины информационной безопасности Российской Федерации, призванная ответить на вызовы современной геополитической и технологической обстановки. Он отметил, что западные ИТ-компании все чаще используются как инструмент деструктивного воздействия, от компьютерной разведки до формирования общественного мнения. Особое внимание в новой доктрине уделяется принципу «безопасность по умолчанию»: защита должна закладываться на этапе проектирования цифровых продуктов, особенно в сфере ИИ. Также усиливается роль государственно-частного партнерства: без участия коммерческих компаний обеспечить безопасность масштабной цифровой инфраструктуры невозможно.

Александр Неверовский, заместитель Государственного секретаря Совета Безопасности Республики Беларусь, рассказал о реализации Концепции информационной безопасности Союзного государства, принятой в 2025 году.

Неверовский сообщил, что в рамках реализации указа президента Республики Беларусь от 14 февраля 2023 года №40 «О кибербезопасности» страны продолжают работу по развитию национальной сети профильных центров кибербезопасности с круглосуточным режимом работы.

Также он добавил, что в 2025 году в Беларуси снизилось число киберпреступлений на 6%, усилена защита финансовой системы, введен запрет на внебиржевые операции с криптовалютами, а также созданы механизмы быстрой блокировки фишинговых сайтов и мошеннических номеров. Он предложил рассмотреть возможность проведения совместных киберучений Союзного государства по аналогии с военными маневрами «Запад-2025».

Валерий Семериков, заместитель генерального секретаря ОДКБ, сообщил, что организация завершила 16-й цикл операции «Прокси», в ходе которой было выявлено и заблокировано более 400 тыс. деструктивных интернет-ресурсов, возбуждено свыше 300 тыс. уголовных дел.

Другие ключевые темы, которые были затронуты на форуме:

- приоритеты развития информационной безопасности России;
- актуальные угрозы информационной безопасности и новые решения в сфере безопасности КИИ;
- искусственный интеллект и информационная безопасность;
- международная информационная безопасность: центральные проблемы и решения;
- доверенные ПАКи: опыт разработки, внедрения, проблемные вопросы;
- умный и безопасный город в современных условиях.

9. Б**изнес-полезность: 4/5**

Опрос участников от журнала RUБЕЖ в рамках форума показал, что основная цель участия в выставке форума — имиджевая (подтверждение статуса компании как участника национальной ИБ-повестки). Второй по значимости мотив — поиск партнеров для совместных проектов в сфере импортозамещения. Поиск прямых клиентов оказался менее востребованным, что типично для мероприятий с доминирующей государственной повесткой.

10. В**ау-эффекты и шоу-элементы: 2/5**

«Инфофорум» выдержан в деловом формате, который не требует зрелищности. Единственным событием, выходящим за рамки стандартной конференции, стала XXIII церемония вручения профессиональной премии «Серебряный кинжал», учрежденной в 2004 году для признания вклада в развитие безопасного информационного общества.

В 2026 году лауреатами Профессиональной премии в области обеспечения информационной безопасности «Серебряный кинжал» стали:

1. В номинации «За вклад в укрепление системы обеспечения информационной безопасности Российской Федерации»:

- **Жуков Юрий Вячеславович,** советник департамента вопросов безопасности в информационной сфере аппарата Совета Безопасности Российской Федерации;
- **Овчинников Денис Васильевич,** начальник Управления заказов по совершенствованию технической основы системы управления Вооруженными Силами Российской Федерации;
- **Ближенский Валерий Витальевич,** начальник отдела Управления ФСТЭК России по Северо-Западному федеральному округу.

1. В номинации «Цифровая трансформация и информационная безопасность» победил **Маслов Владимир Андреевич,** директор Департамента цифровых технологий Торгово-промышленной палаты Российской Федерации.
2. В номинации «За информационную безопасность перспективных технологий» победил **Служеникин Дмитрий Игоревич,** секретарь Консорциума исследований безопасности технологий искусственного интеллекта.
3. В номинации «За вклад в развитие международного сотрудничества в сфере информационной безопасности» **обладателем Почетного диплома премии «Серебряный кинжал» стал** **Баньковский Алексей Леонидович,** начальник управления Государственного секретариата Совета Безопасности Республики Беларусь.

Отсутствие интерактивных демозон, технологических инсталляций или арт-проектов (в отличие от Sfitex с его галереей «Пожара не будет») уводит с мероприятия широкую отраслевую аудиторию. Но не целевых специалистов. С другой стороны - зрелищная подача приличествует в нынешних реалиях на самых крупных формумах с участием первых лиц государтва. Зачастую именно она усиливает убедительность тезисов и стратегем, звучащих в докладах.

- На ПМЭФ и ПЭФ используют масштабные LED-инсталляции, AR-визуализации ключевых проектов и интерактивные стенды, где высокопоставленные чиновники демонстрируют цифровые двойники регионов или инфраструктурных объектов.

- ЦИПР ежегодно выстраивает пространство вокруг тематических зон - от «Цифрового правительства» до «Безопасного города» - с живыми кейсами, иммерсивными симуляторами кибератак и демонстрацией работы ситуационных центров в реальном времени.

Именно поэтому организаторам “Инфофорума” имеет смысл посмотреть в сторону инструментов эмоциаональной окраски мероприятия на будущее. Мероприятие и выступления государственных служащих от этого только выиграют.

11. Транспортная доступность: 5/5

Площадка проведения форума в кластере «Ломоносов» расположена в 15 минутах пешком от станции метро «Раменки» и в 10 минутах до станции метро «Университет». Также рядом находится остановка общественного транспорта и парковка на 245 мест.

Уже не первое мероприятие в кластере оправдывает такой выбор места проведения. Одним из первых эффективность площадки опробовали организаторы [форума «Безопасность. Сделано в России»](https://ru-bezh.ru/videos/sb-forum-obzor) еще в 2023 году.

12. Медийность и инфопартнеры: 5/5

«Инфофорум-2026» получил значительное медиаосвещение: организаторы заявили участие около 300 представителей СМИ, включая федеральные агентства (ТАСС, РИА Новости), деловые издания (РБК, «Ведомости», «Коммерсантъ»), профильные СМИ («Хакер»), а также телеканал «Звезда». Отраслевой информационный партнер — журнал RUБЕЖ.

Технически PR-обеспечение также было на высоком уровне: все ключевые сессии, включая пленарное заседание, транслировались онлайн.

13. Общая организация и безопасность: 4/5

Безопасность мероприятия обеспечена на высоком уровне: доступ к залам был строго привязан к типу аккредитации (участник, спикер, пресса, онлайн-участник). Охрана присутствовала у всех входов и в ключевых точках перемещения, но при этом не создавала ощущения избыточного надзора, работа персонала была ненавязчивой и профессиональной.

Зонирование пространства также заслуживает высокой оценки. Конференц-залы («Молекула», «Физика», «Атом») были четко отделены от выставочной экспозиции, расположенной в фойе и на двух этажах. Между ними были организованы зоны нетворкинга с комфортной мягкой мебелью, что позволяло участникам не только обсуждать услышанное на сессиях, но и проводить деловые встречи в неформальной обстановке. Навигация по площадке была интуитивно понятной: указатели с названиями залов и программой размещались на каждом этаже.

Чистота и порядок поддерживались на протяжении всех двух дней форума. Ни в залах, ни в зонах общего пользования не наблюдалось скопления мусора или пустых кофейных стаканчиков.

Главный организационный сбой произошел в сфере кейтеринга. В первый день, в обеденный перерыв, возникла очередь из более чем 50 человек к единственной точке выдачи горячего питания. Организаторы явно не рассчитали количество порций, и часть участников осталась без обеда, что косвенно указывает на нескоординированность системы регистраций на форум и планирования работы сервисных служб.

В то же время кофе-брейки были организованы качественно: в течение дня в фойе постоянно работали точки с кофе и чаем.

Заключение

«Инфофорум-2026» стал особенно ценен для компаний, работающих в сегменте КИИ и госзаказа. Здесь были озвучены конкретные требования регуляторов, дорожные карты сертификации и приоритеты закупок на 2026 год по таким направлениям, как:

- **искусственный интеллект и безопасность.** Отдельная сессия была посвящена не только рискам, но и разбору атак с использованием ИИ, защите от дипфейков и автоматизации тестирования;
- **квантовые технологии.** Появилась отдельная детализированная сессия, охватывающая постквантовую криптографию, отечественные стандарты, квантовый ИИ и подготовку кадров.

Также в программу 2026 года добавлены специализированные сессии по сетевой безопасности с анализом российских NGFW, DLP, SIEM и «Умному и безопасному городу» с акцентом на ИИ, биометрию и мобильные сервисы.

Важно: регуляторы выбирают «Инфофорум» для подведения результатов работы отрасли информбезопасности за год. Форум 2026 года стал площадкой для презентации важнейших отраслевых данных. Например, ФСТЭК представила итоги проверок объектов КИИ, выявив, что лишь 36% из них достигли минимального уровня защиты.

С индексом 4,3 «Инфофорум-2026» демонстрирует стабильность и авторитет, но требует развития в части:

- усиления практической демо-компоненты: не просто расширить площадь экспозиции, а, скорее, сделать акцент на демонстрации новых продуктов и live-демонстрациях, а не только на информационных стендах;
- создания полноценной медиазоны: необходимо организовать пресс-центр с рабочими местами для журналистов, зоной брифингов и технической поддержкой для оперативного освещения ключевых инфоповодов;
- развития эмоциональной и визуальной составляющей мероприятия с учетом поколенческих особенностей специалистов в сфере технологий. Интерактивные демозоны, визуализация киберугроз в реальном времени, AR/VR-инсталляции, видеоряды с кейсами защиты КИИ — все это более полно реализует кадровый потенциал отрасли ИБ.

Читайте также: Кибератак на бизнес через уязвимости в бухгалтерии [стало больше](https://ru-bezh.ru/kompanii-i-ryinki/news/26/02/01/moshenniki-atakuyut-biznes-cherez-uyazvimosti-v-buhgalterii).

Благодарим за оставленный Вами отзыв! Мы стараемся становиться лучше!