

Актуальные вопросы подготовки кадров по информационной безопасности



Академия
Информационных
Систем



Смотри в будущее. Инвестируй в знания.



Хайров Игорь Евгеньевич

Заместитель директора
Академии Информационных Систем,
кандидат технических наук

Продукты и услуги



Дополнительное
профессиональное
образование
и профпереподготовка



Организация конференций,
форумов, выездных
мероприятий



Организация вебинаров,
семинаров, митапов

Академия в цифрах

28 лет в сфере профессионального образования

300+

образовательных программ

100 000 +

человек прошло обучение

50

преподавателей, экспертов-практиков

700

корпоративных заказчиков



Основные направления деятельности

Информационная
безопасность



Информационные
технологии



Корпоративная
безопасность



Электронный
документооборот



Импортозамещение



Выездное обучение



**Опрос по актуальным проблемам
обучения, повышения
квалификации и осведомлённости
сотрудников в области
информационной безопасности.**

Цель опроса –

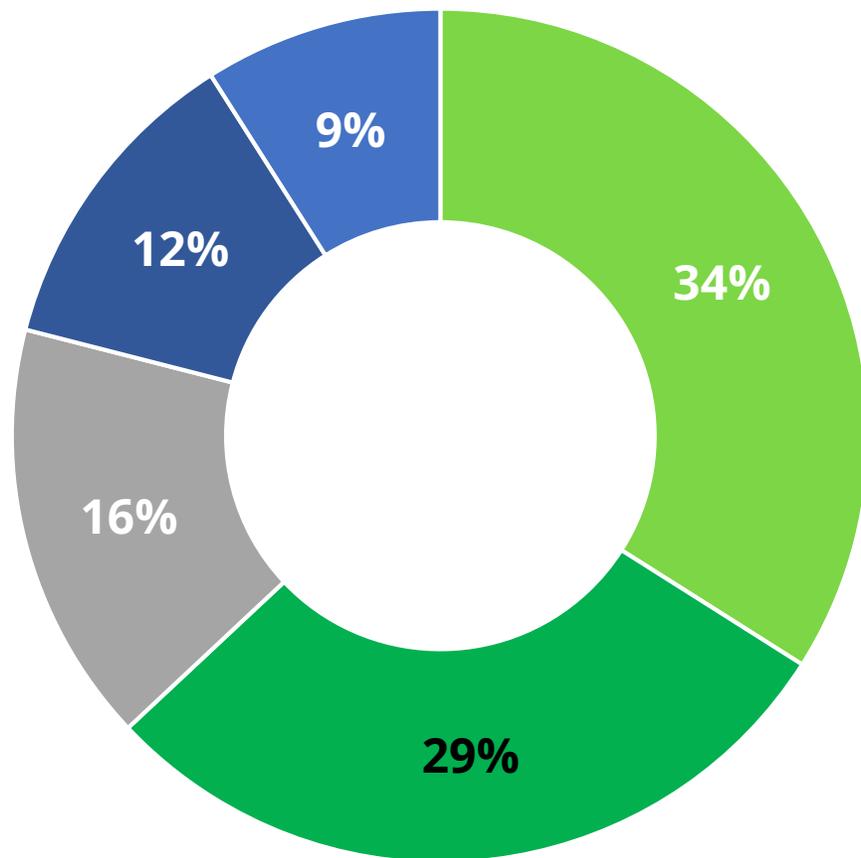
- Выявить текущее состояние профессиональной подготовки и уровень осведомлённости сотрудников организаций в сфере ИБ
- Определить ключевые кадровые проблемы и потребности в дополнительном профессиональном обучении
- Сформировать рекомендации по совершенствованию кадровой политики и образовательных программ в области ИБ

Отрасли экономики и география
расположения организаций (субъекты РФ) –
не делалось ограничений;

Количество респондентов – более 80
представителей организаций,



Ваша текущая должность

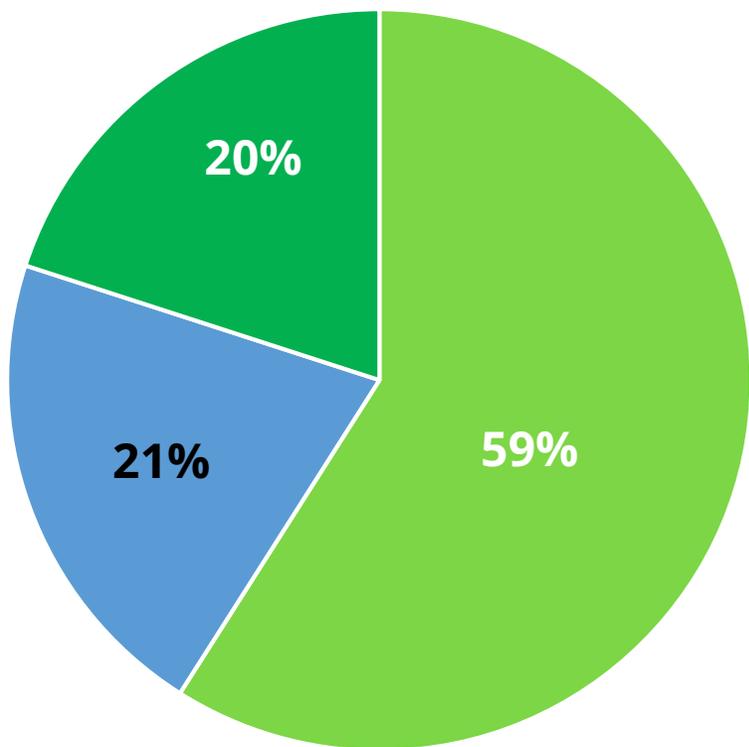


- Специалист / инженер по ИБ
- ИТ-специалист (администратор, разработчик и пр.) с функциями ИБ
- Другая (не ИТ и не ИБ) должность с функциями ИБ
- Аналитик ИБ
- Руководитель подразделения ИБ

Выводы:

Основную группу составляют **специалисты и инженеры по ИБ (34%)** и **ИТ-специалисты с функциями ИБ (29%)**. Это говорит о том, что ответственность за ИБ зачастую совмещается с другими обязанностями, и специалистов, полностью посвященных ИБ, относительно немного.

Как вы оцениваете текущий уровень профессиональной подготовки сотрудников по ИБ в вашей организации?



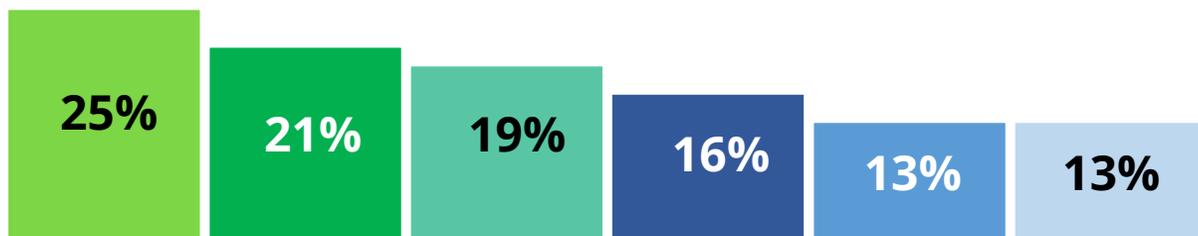
- Средний, требует повышения квалификации и развития практических навыков
- Низкий, требуется срочная переподготовка и принятие срочных мер
- Высокий, соответствует вызовам

Выводы:

59% респондентов оценивают уровень подготовки сотрудников как средний, что свидетельствует о значительных возможностях и необходимости дальнейшего профессионального развития и обучения. Критически низкий уровень подготовки отмечают **21%**.

На ваш взгляд, каких компетенций сотрудникам чаще всего не хватает в сфере ИБ? (Выберите до 3 вариантов)

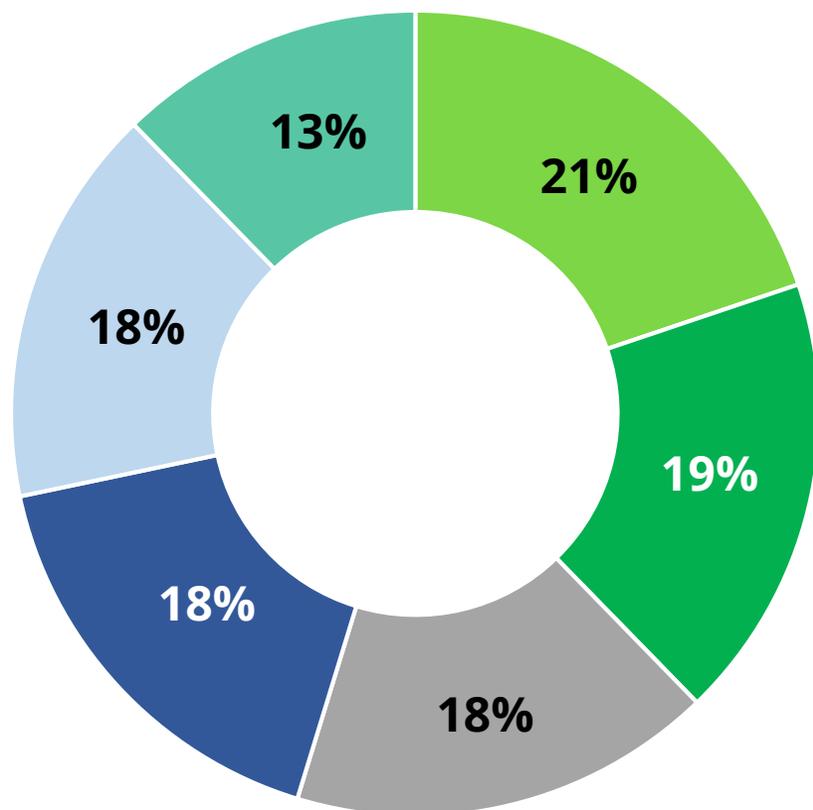
- Технические навыки (сетевые технологии, инфраструктура, администрирование, киберполигоны)
- Знания современных угроз и методов защиты
- Стратегическое мышление и планирование в сфере ИБ
- Навыки коммуникаций и взаимодействия с другими подразделениями
- Знания нормативно-правового регулирования (законы, стандарты)
- Методологические навыки (оценка рисков, разработка политик)



Выводы:

Наиболее остро не хватает технических навыков (**25%**), а также знаний современных угроз (**21%**) и стратегического мышления (**19%**). Также важны навыки коммуникации (**16%**).

Какие форматы обучения вы считаете наиболее эффективными для сотрудников ИБ?



- Очные курсы, семинары, практические мастер-классы
- Обучение по индивидуальным планам и наставничество (менторство)
- Онлайн-курсы, вебинары, дистанционные тренинги
- Участие в конференциях, форумах, профильных мероприятиях
- Внутренние корпоративные тренинги и обучение
- Самостоятельное изучение (литература, статьи, исследования)

Вывод

Наиболее востребованы очные курсы и мастер-классы (**21%**), а также наставничество (**19%**), что говорит о необходимости совмещать теорию и практику с персональным подходом.

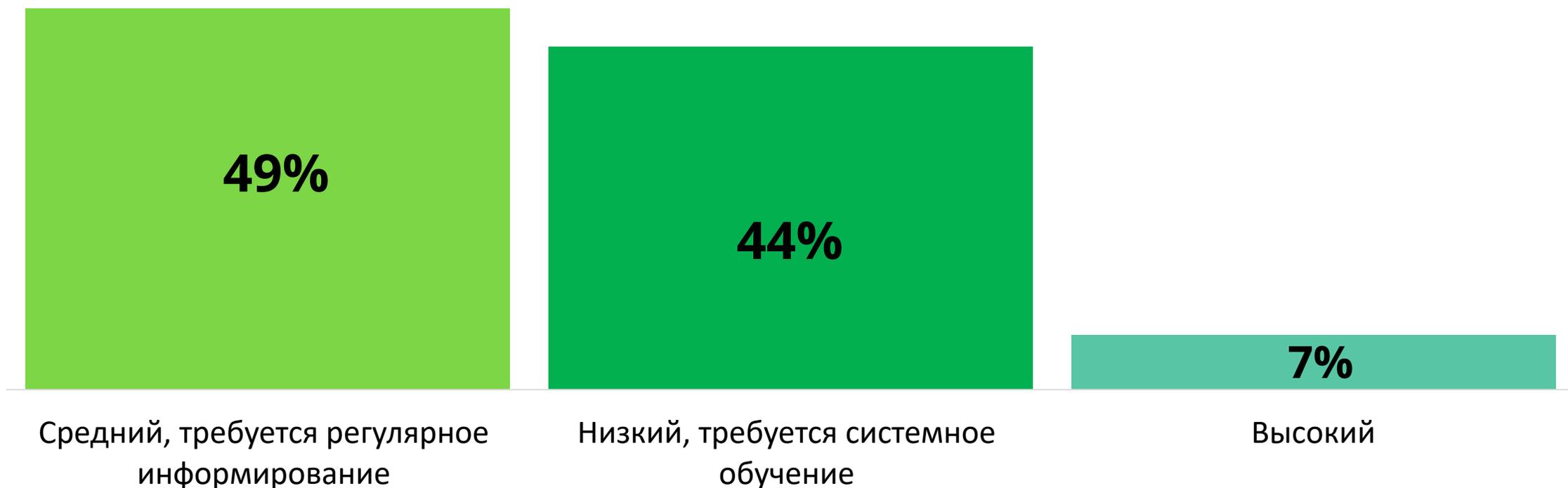
Какие сложности чаще всего возникают при освоении новых знаний и навыков в области ИБ?



Вывод

Главные сложности: нехватка времени (**22%**), отсутствие практического опыта (**19%**) и нехватка квалифицированных преподавателей (**19%**).

Как вы оцениваете уровень осведомленности по вопросам ИБ сотрудников, не связанных напрямую с ИТ и ИБ



Вывод

Осведомленность низкая (**44%**) или средняя (**49%**), что требует системного подхода к обучению всех категорий сотрудников.

Какие форматы повышения осведомленности по ИБ для всех категорий сотрудников наиболее эффективны в вашей организации?



Вывод

Наиболее эффективны примеры реальных инцидентов (**24%**), очные тренинги (**20%**) и игровые форматы (**19%**).

Итоговые выводы и рекомендации по кадровой политике

Кадровые вызовы:

- **Недостаточная специализация** сотрудников в сфере ИБ.
- **Средний и низкий уровень** подготовки значительной части сотрудников.
- **Низкая регулярность обучения**, слабая осведомленность сотрудников.



Итоговые выводы и рекомендации по кадровой политике

Рекомендации по кадровой политике для организаций:

- **Внедрение регулярного обучения и аттестации** сотрудников всех категорий.
- Создание **систем наставничества и практического опыта** через стажировки и киберполигоны.
- Увеличение бюджетов **и стимулирование сотрудников к постоянному обучению.**



Итоговые выводы и рекомендации по кадровой политике

Рекомендации по дополнительному профессиональному обучению:

- **Для сотрудников ИБ:** сосредоточить усилия на практической составляющей, технической подготовке, нормативно-правовом обучении и социальной инженерии.
- **Для всех категорий сотрудников (не ИТ и не ИБ):** системное обучение через регулярные информационные мероприятия, игровые и интерактивные форматы, а также разбор реальных инцидентов.

Актуальность обучения

Можно выделить пять крупных категорий аудитории, кого нужно учить вопросам обеспечения информационной безопасности:

1. Руководители органов (организаций);
2. Заместители руководителей органов (организаций) по ИБ (в трактовке Указа Президента РФ №250);
3. Специалисты по информационной безопасности, работники структурных подразделений, обеспечивающих ИБ органа (организации);
4. Техники по защите информации;
5. Сотрудники организаций, не связанные с обеспечением ИБ в организации.



Актуальность обучения

Для первой категории «**Руководители органов (организаций)**» достаточно курсов повышения квалификации для понимания проблематики, «масштабов бедствия» при нарушениях ИБ, вопросов ответственности и т.п.



Рассматриваемые вопросы:

- Организационное обеспечение ИБ;
- Законодательство, нормативные акты, положения, политики и инструкции в области ЗИ;
- Управление информационной безопасностью;
- Ответственность за нарушение правил ИБ;
- Риски информационной безопасности;
- Элементы защиты и технологии защиты
- Коммерческая тайна в системе обеспечения безопасности;
- Алгоритмы расследования инцидентов информационной безопасности;
- Элементы киберучений для руководящего состава.



Курс для руководителей:
«Информационная
безопасность, как часть
комплексной безопасности
организации» (2 дня, 16 часов)



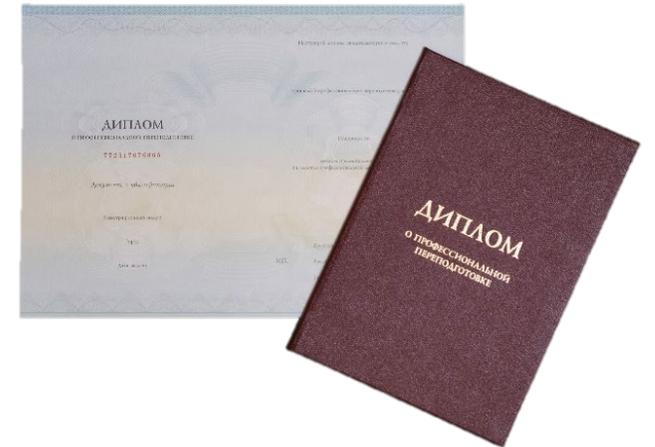
Актуальность обучения



Для второй категории «**Заместители руководителей органов (организаций) по ИБ**» однозначно трактуется обязательность обучения на курсах профессиональной переподготовки по ИБ (при отсутствии профильного образования по ИБ).

-  **520 часов.** «Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и некриптографическими методами»
-  **504 часа.** «Информационная безопасность. Техническая защита конфиденциальной информации»
-  **502 часа.** «Информационная безопасность. Безопасность значимых объектов критической информационной инфраструктуры»

Диплом о профессиональной переподготовке



Актуальность обучения

1. Курсы согласованы ФСТЭК России и/или ФСБ России, согласно требованиям Приказа Минобрнауки России №1316.
2. Продолжительность более 500 часов, что подходит и для гос.гражданских служащих (согласно Указа Президента РФ №68) и для лицензиатов ФСБ России и ФСТЭК России.
3. Программы курсов состоят из базовой и вариативной частей.

Базовая часть включает в себя вопросы:

- Нормативно-правовые основы обеспечения ИБ в РФ;
- Объекты защиты информации, меры и средства защиты информации;
- Обеспечение безопасности информации ограниченного доступа, включая защиту ПДн при их обработке в ИСПДн;
- Обеспечение безопасности объектов КИИ;
- Построение комплексной системы обеспечения ИБ органа (организации);
- Системы управления ИБ и обеспечения непрерывности бизнеса. Управление проектами по ИБ;
- Вопросы обнаружения, предупреждения и ликвидации последствий компьютерных атак. Реагирование на инциденты ИБ;
- Техническая защита информации от утечки по техническим каналам;
- Защита информации ограниченного доступа с использованием шифровальных (криптографических) средств.

Вариативная часть необходима для учета потребности конкретного заказчика образовательных услуг, отраслевых и региональных особенностей, должностных категорий и групп должностей обучающихся.



Актуальность обучения



Для третьей категории «**Специалисты по информационной безопасности, работники структурных подразделений, обеспечивающих ИБ органа (организации)**» спектр курсов обширен и зависит от их квалификации и используемых в организации СЗИ. **Курсы согласованные ФСТЭК России:**

-  **106 часов.** «Информационная безопасность»
-  **112 часов.** «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов КИИ»
-  **80 часов.** «Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, на базе операционной системы специального назначения ASTRA LINUX SPECIAL EDITION»
-  **80 часов.** «Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну в сфере здравоохранения»

Удостоверение о повышении квалификации



Программа повышения квалификации

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Программа курса согласована ФСТЭК России



Актуальность обучения (один из аспектов)



В 2023г.

Территориальными органами проведено 2 плановых контрольных (надзорных) мероприятия, 3510 контрольных (надзорных) мероприятий, осуществляемых без взаимодействия с проверяемым лицом и 49 внеплановых КНМ (в том числе по требованиям органов прокуратуры).

Основаниями для проведения внеплановых контрольных (надзорных) мероприятий, послужили указания центрального аппарата Роскомнадзора, данные на основании имеющихся сведений о совершённых или готовящихся нарушениях.

Общее количество лиц, в отношении которых проведены КНМ – 5999.

В деятельности 4022 контролируемых лиц выявлены нарушения (типичные нарушения приведены в Докладе).



Приказ Роскомнадзора № 53
29.03.2024

**«Доклад о правоприменительной
практике организации
и проведения федерального
государственного контроля
(надзора) за обработкой
персональных данных в 2023г».**



Актуальность обучения

Для третьей категории «**Специалисты по информационной безопасности, работники структурных подразделений, обеспечивающих ИБ органа (организации)**» спектр курсов обширен и зависит от их квалификации и используемых в организации СЗИ.



и многие другие



Актуальность обучения

Мероприятия, необходимые для всех должностей, занимающихся вопросами обеспечения информационной безопасности, в том числе обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты:

1. Программы повышения осведомленности по вопросам ИБ (включая геймификацию)
2. Проведение практических учений по противодействию компьютерным атакам
3. Вебинары по информационной безопасности
4. Самостоятельное изучение вопросов по ИБ.
5. Повышение квалификации по вопросам обеспечения информационной безопасности
6. Участие в профильных мероприятиях по ИБ.





Деловые мероприятия Академии Информационных Систем

Организация деловых мероприятий

Академия Информационных Систем –организатор конференций, форумов и круглых столов.

Наши мероприятия проходят при поддержке и активном участии государственных ведомств, регуляторов, ассоциаций и общественных организаций, ученых и экспертов-практиков.

25 лет

в сфере организации деловых мероприятий

15 000+

участников ежегодных деловых событий

7 000+

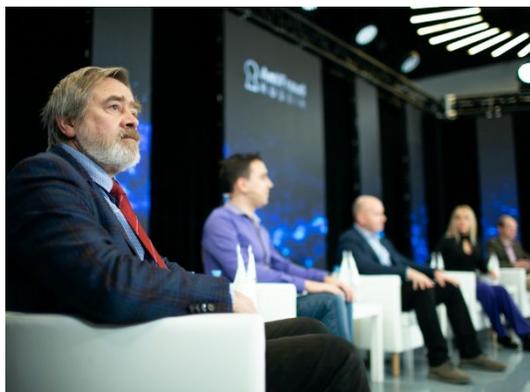
докладов и выступлений в рамках конференций

170+

успешно проведенных мероприятий



Ежегодно мы организуем более 12 деловых мероприятий



Также мы:

- Проводим корпоративное обучение,
- Создаем программы под заказчика,
- Готовим к сдаче сертификационного тестирования,
- Делаем выездное обучение и мероприятия,
- Проводим тестирование и сертификацию на соответствие профстандартам в области ИБ и платежных систем.

Среди наших довольных клиентов: Вертолеты России, АО «Гознак», Государственная корпорация «Ростех», КАМАЗ, Газпром, Оборонэнерго, Федеральная нотариальная палата, ФЦИИТ и много других российских компаний.



Ростех



ВЕРТОЛЕТЫ РОССИИ





Присоединяйтесь к нашим соцсетям!



**Telegram-канал
АИС**



**Яндекс. Дзен
АИС**



Rutube АИС



**Постоянный
репозиторий по Python**



**Telegram-канал
«ВсёпроЭДО»**



**Telegram-канал
КРЭБ**



**Telegram-канал
AntiFraud Russia**



**Telegram-канал
МедИнфоБез**

Спасибо за внимание!

Хайров Игорь, АИС

+7(495) 120-04-02 | info@infosystem.ru | www.infosystems.ru; www.vipforum.ru