НАЦИОНАЛЬНОЕ ОБЪЕДИНЕНИЕ
СПЕЦИАЛИСТОВ ПО БЕЗОПАСНОСТИ БИЗНЕСА

7 часов CPE

IX ЕЖЕГОДНАЯ ОНЛАЙН-КОНФЕРЕНЦИЯ

18 марта 2026г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЗГЛЯД ИЗНУТРИ КОМПАНИИ

Обеспечение информационной безопасности и непрерывности бизнеса в условиях экономической войны против России

В ПРОГРАММЕ КОНФЕРЕНЦИИ

- Комплексный подход к обеспечению информационной безопасности организации
- Внутренний аудит и информационная безопасность. Есть ли шансы у внутренних аудиторов?
- Искусственный интеллект в информационной безопасности: облегчит ли он жизнь до невыносимой легкости бытия?
- Главные ошибки в организации системы информационной безопасности
- Проведение расследований инцидентов в ИБ: правовые аспекты, которые необходимо учитывать
- Проведение интервью с сотрудниками ИТ: психологические особенности ИТ-специалистов
- Социальная инженерия. Эффективные методы противодействия. Программа по противодействию СИ в организации
- Это должен знать каждый: технология социальной инженерии. Как проектируют атаки на вашу ИБ
- Перспективы достижений и провалов в области ИБ в ближайшие годы

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ: ДИРЕКТОР ПО БЕЗОПАСНОСТИ www.s-director.ru

Ассоциация «Объединение сертифицированных специалистов по расследованию хищений»

www.acfe-rus.com ■ info@acfe-rus.org ■ +7 (495) 728-76-10

09:15 - 09:25 Подключение.

09:25 - 09:30 Приветствие. Открытие конференции.

09:30 - 10:00 **Сергей Мартынов**

Президент Национального объединения специалистов по безопасности бизнеса.

Эволюция ИБ и ИБ эволюции: точка пересечения процессов и чего ожидать дальше.

Если под эволюцией человека понимать развитие его интеллекта, то пик её был пройден в 30 годы прошлого века. «Схема Долиной» показала не только коррупцию системы правосудия, но и прогрессирующую деградацию интеллекта общества в целом.
Сегодня ИБ – это не только защита информации компании от утечки, но также защита сотрудников от потока входящей извне информации. Политика «осажденной крепости» в ИБ. От чего защищать персонал информационно?
Дам несколько конкретных советов, которые позволят постелить соломки там, куда неизбежно придется падать.

10:00 - 10:30 **Георгий Гусляев**

Независимый эксперт по ИБ.

Когда информационной безопасности достаточно? Сколько она стоит?

Вечный вопрос «сколько нужно?» Почему это сложно оценить?
Что значит «достаточно»? Критерии достаточности ИБ.
Из чего складывается стоимость ИБ? Как оценить необходимый бюджет.
Когда ИБ «перезащищена» и «недозащищена»? Как определить «золотую середину»?
Примеры из практики.

10:30 - 11:00 **Михаил Хавин**

Руководитель службы информационной безопасности, Аскона.

Перспективы достижений и провалов в области ИБ в ближайшие годы.

Сложности и опасности прогнозирования.
Опасности, продуцируемые самими людьми.
Опасности, продуцируемые производителями решений.
Новые инструменты ИБ.
Изменения и родовые проблемы ИТ систем.
Меры противодействия.

11:00 - 11:30 **Обсуждение. Ответы на вопросы.**

11:30 - 11:45 **Перерыв.**

11:45 - 12:15 **Антон Грунтов**

Директор по безопасности группы компаний Eqvanta.

Кто все эти люди, где и почем их взять?

По некоторым оценкам уровень атак на российские компании в 2025-м году вырос в четыре раза по сравнению с предыдущим годом. При этом многие компании, озаботившиеся собственной киберзащитой, столкнулись с проблемой набора сотрудников в подразделения ИБ. Кто-то впервые столкнулся с такой новой формой как кадровый экстремизм на основе т.н. «осознанной меркантильности». Своей практикой поиска, отбора сотрудников, их развития и увольнения поделится эксперт и бизнес - тренер BSP Грунтов Антон

12:15 - 12:45 **Оксана Павленко**

Психолог-полиграфолог.

Проведение интервью с сотрудниками ИТ: психологические особенности ИТ-специалистов.

Особенности рынка труда в IT-сфере;
Ключевые черты личности IT-специалистов, их мотивация;
Лайфхаки и секреты интервью с программистами и разработчиками;
Оценка и предотвращение возможных риск-факторов в деятельности IT-специалистов;
Реальные кейсы и рекомендации по работе с данной категорией персонала.

12:45 - 13:05 **Обсуждение. Ответы на вопросы.**

13:05 - 14:00 **Перерыв на обед.**

14:00 - 14:30 **Александр Отогочёв**

Независимый эксперт, член Национального объединения специалистов по безопасности бизнеса.

Внедрение искусственного интеллекта в бизнес-процессы по противодействию мошенничества: вызовы информационной безопасности.

Искусственный интеллект формирует глобальную технологическую революцию, напрямую влияя на безопасность финансовых систем и борьбу с преступлениями. Рынок ИИ оценивается в триллионы долларов, а более 70% российских компаний уже используют генеративный ИИ.
Внедрение ИИ в антифрод-системы, мониторинг и финансовые расследования — это уже реальность. Но вместе с возможностями возникают и новые угрозы: «галлюцинации» моделей, утечки данных, атаки на облачные хранилища. Ключевой вопрос: как не стать заложником технологий и сохранить надёжный контур безопасности бизнеса?

14:30 - 15:00 Анатолий Килячков

Старший эксперт компании «Б1-консалт.

Риски использования больших языковых моделей.

В выступлении будут рассмотрены риски, органически присущие большим языковым моделям (LLM), которые являются прямым следствием принципа их работы и обусловлены внутренней структурой, способом построения, обучения и функционирования LLM.
Рассмотрим следующие риски и способы их минимизации:
1. Риск взлома больших языковых моделей.
2. Риск галлюцинаций.
3. Языковой bias.
4. Риск ошибок в общении с LLM.
5. Риск неправильного дообучения (думскролинг).

15:00 - 15:20 Обсуждение. Ответы на вопросы.

15:20 - 15:35 Перерыв.

15:35 - 16:05 Светлана Зуева

Руководитель отдела рисков ИБ и аудита,ООО "ГК "Иннотех".

Внутренний аудит и информационная безопасность. Есть ли шансы у внутренних аудиторов.

Человеческий фактор и мифы - что можно и что не стоит говорить внутренним аудиторам?
Можно ли автоматизировать процесс внутреннего аудита?
ИИ, сможет ли он помочь внутренним аудиторам делать свою работу лучше?

16:05 - 16:35 Вадим Белозеров

Эксперт Центра Развития Комплаенс Контроля.

Социальная инженерия. Эффективные методы противодействия. Программа по противодействию СИ в организации.

Что такое СИ как риск: типовые сценарии и точки уязвимости бизнеса?
«Защитные правила», которые дают результат сразу после внедрения.
Как выстроить программу противодействия СИ?
Как измерять эффективность системы противодействия?
Какой должна быть реакция на инциденты?

ЗАРЕГИСТРИРОВАТЬСЯ

16:35 - 17:05 Дмитрий Иванов

SA WEST, Партнер.

А не слишком ли много я о себе рассказываю? Как помочь владельцам бизнеса находить баланс между публичным имиджем, индивидуальным брендом и угрозами для себя лично и своей компании.

В самом конце 2025 года на меня неожиданно свалилось несколько проектов, в которых рефреном звучал один и тот же вопрос заказчика: «А не слишком ли много я о себе рассказываю?».
Раньше подобные запросы сводились к классической задаче: собрать информацию о чувствительных данных, циркулирующих в сети, оценить угрозы публичной репутации, проверить упоминания заказчика в «файлах», документах, отчетах и списках. Это были проекты относительно скучные, о них и рассказывать неинтересно.
Сегодня ситуация изменилась: индивидуальный бренд и публичный имидж становятся обязательным условием формирования доверия между провайдером и клиентом, а в некоторых случаях и между публичным бизнесом и его акционерами. Часто выигрывает тот, кто максимально открыт, эпатажен, вызывающе откровенен.
Но где заканчивается продуманная открытость и начинается бесконтрольное распространение чувствительной информации с целью завоевать клиента, рынок, инвесторов или удовлетворить ожидания акционеров? Когда публичность становится неоправданным риском для личной и корпоративной безопасности?

17:05 - 17:35 Обсуждение. Ответы на вопросы.

17:35 - 17:40 Итоги и завершение конференции.

ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ

Проведение ежегодной конференции по информационной безопасности вошло в добрую традицию.

Наша конференция - это уникальная возможность встретиться с коллегами, обсудить насущные вопросы, поделиться опытом и идеями.

На конференции выступят как докладчики, работающие в отделах информационной безопасности, так и сотрудники контролирующих служб крупных и средних компаний.
Конференция будет полезной для сотрудников служб безопасности и внутренних аудиторов, которые хотят глубже понять и узнать о системе ИБ, современных угрозах, способах защиты; а также для специалистов ИБ для обмена опытом с коллегами.

Участники конференции получат сертификаты установленного образца с указанием **CPE часов.**

Срок регистрации - до 15 марта 2026г.
Срок оплаты - до 17 марта 2026г.

СТОИМОСТЬ УЧАСТИЯ*:
45 тыс. рублей (100% предоплата, счет-оферта). По данной стоимости может участвовать до 3-х сотрудников от одной организации.

Специальная цена для членов нашей ассоциации:
7 тыс. рублей.
*- НДС не облагается.

По не зависящим от организатора причинам в программе могут быть незначительные изменения