ФИНКОНТ
учебный центр

+7 (495) 698-63-64
8 (800) 234-55-22

seminar@finkont.ru
www.finkont.ru

Информационная безопасность в организациях: изменения законодательства и измерения эффективности (40 часов очно + 32 часа заочно)

В 2022 году были принято большое количество нормативно-правовых нововведений сфере информационной безопасности (Указы Президента РФ от 03.05.2022 № 252, №250, №203, Информационное сообщении ФСТЭК от 11.04.2022 №240/24/1950, от 25.03.2022 №240/13/156). Кроме того, в марте 2021 года изменились правила работы с персональными данными: с 1 марта вступили в силу изменения в Федеральный закон «О персональных данных», которыми вводится новое понятие «персональные данные, разрешенные для распространения», определяются особенности обработки таких данных и регламентируются новые требования к оператору персональных данных, а с 27 марта вступили в силу поправки к КоАП РФ, которыми значительно увеличены существующие и введены новые штрафы за нарушения правил обработки персональных данных.

Дата проведения: Открытая дата

Вид обучения: Курс повышения квалификации

Формат обучения: Дневной

Срок обучения: 5 дней

Продолжительность обучения: 72часа

Место проведения: г. Москва, ул. Золотая, д. 11, бизнес-центр «Золото», 5 этаж. Всем участникам высылается подробная схема проезда на семинар.

Для участников предусмотрено: Методический материал, кофе-паузы.

Документ по окончании обучения: По итогам обучения слушатели, успешно прошедшие итоговую аттестацию по программе обучения, получают Удостоверение о повышении квалификации в объеме 72 часов (в соответствии с лицензией на право ведения образовательной деятельности, выданной Департаментом образования и науки города Москвы).

Для кого предназначен

Юристов, руководителей и специалистов отдела кадров, работников, назначенных ответственными за организацию обработки персональных данных (DPO), руководителей и специалистов служб безопасности, специалистов по информационной безопасности, руководителей организаций.

Цель обучения

Получить системные и актуальные представление о системе законодательных требований в области информационной безопасности, комплексе мероприятий по её измерению и культуре реализации.

Особенности программы

Указаны даты очной части обучения.
На-курсе будет проведен анализ типовых нарушений законодательства в-области информационной безопасности, даны практические рекомендации, как минимизировать риски и-избежать эти нарушения, как провести измерения информационной безопасности, рассмотрены новые правила предоставления информации ФСТЭК России и-проведения надзорных проверок

Роскомнадзора.
Обучение проводится в-очно-заочной форме с-применением дистанционных технологий и-включает 40-часов очного общения с-экспертами и-коллегами или формат онлайн-трансляции, включая практические занятия, деловые игры. В-рамках заочной части обучения слушатели получают доступ к-информационно-образовательной среде учебного центра «Финконт», включающей презентации материала, учебно-методические материалы, задания и-тесты для проверки знаний.
По-окончании обучения и-успешного прохождения тестирования **выдается удостоверение о-повышении квалификации установленного образца.**

Это мероприятие можно заказать в корпоративном формате (обучение сотрудников одной компании).

Программа обучения

ПРОГРАММА ОБУЧЕНИЯ (очная часть).

День-1. «Актуальные изменения государственной политики России в-сфере информационной безопасности».

- Указ Президента Российской Федерации от-03.05.2022 №-252 «О-применении ответных специальных экономических мер в-связи с-недружественными действиями некоторых иностранных государств и-международных организаций».
- Указ Президента Российской Федерации от-01.05.2022 №-250 «О-дополнительных мерах по-обеспечению информационной безопасности Российской Федерации».
- Указ Президент Российской Федерации от-14.04.2022 №-203 «О-Межведомственной комиссии Совета Безопасности Российской Федерации по-вопросам обеспечения технологического суверенитета государства в-сфере развития критической информационной инфраструктуры Российской Федерации».
- Информационное сообщении ФСТЭК от-11.04.2022 №-240/24/1950. о-порядке представления документов по-аттестации объектов информации, обрабатывающих информацию ограниченного доступа, не-составляющей государственную тайну.
- Информационное сообщение ФСТЭК России от-25.03.2022 №-240/13/1561-об отмене оплаты государственной пошлины за-госуслуг по-предоставлению лицензии на-деятельность по-технической защите конфиденциальной информации и-лицензии на-деятельность по-разработке и-производству средств защиты конфиденциальной информации до-конца 2022-года.
- Постановление Правительства-24.03.2022 №-448 «Об-особенностях осуществления государственного контроля (надзора), муниципального контроля в-отношении аккредитованных организаций, осуществляющих деятельность в-области информационных технологий, и-о-внесении изменений в-некоторые акты Правительства Российской Федерации».
- Приказ Минцифры от-25.02.2022 №-142 «Об-утверждении формы проверочного листа (списка контрольных вопросов), используемого Министерством цифрового развития, связи и-массовых коммуникаций Российской Федерации при осуществлении федерального государственного контроля (надзора) в-сфере идентификации-и (или) аутентификации».
- Постановление Правительства от-21.02.2022 №-222 «Об-утверждении Правил представления заинтересованным лицам документа о-полномочиях физического лица в-случае, предусмотренном частью 2-статьи 17.1 Федерального закона «Об-электронной подписи».
- Постановление Правительства от-21.02.2022 №-223 «Об-утверждении организационно-технических требований к-порядку хранения, использования и-отмены указанных в-статьях 17.2 и-17.3 Федерального закона „Об-электронной подписи“ доверенностей».
- Постановление Правительства от-21.02.2022 №-224 «Об-утверждении требований к-нормативным правовым актам федеральных органов исполнительной власти, устанавливающим порядок представления доверенности в-предусмотренном пунктом 2-части 1-статьи 17.2 Федерального закона «Об-электронной подписи» случае, и-требований к-порядку представления доверенности в-предусмотренном пунктом 2-статьи 17.3 Федерального закона «Об-электронной подписи».
- Приказ ФСТЭК России от-10.02.2022 №-26-«О-внесении изменений в-Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом Федеральной службы по-техническому и-экспортному контролю от-6-декабря 2017-г. №-227».
- ГОСТ Росстандарта 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к-регистрируемой информации» введен в-действие с-1.02.2022.
- Приказ ФСБ России от-31.01.2022 №-35-«Об-утверждении форм документов, используемых Федеральной службой безопасности Российской Федерации в-процессе лицензирования в-соответствии с-Федеральным законом от-4-мая 2011-г. №-99-ФЗ «О-лицензировании отдельных видов деятельности», который, в-том числе, утверждает оценочные листы, применяемые при осуществлении оценки соответствия соискателей (лицензиатов) лицензионным требованиям, например, на-соответствие ПП-313.
- Положение Банка России от-12.01.2022 №-787-П «Об-обязательных для кредитных организаций требованиях к-операционной надежности при осуществлении банковской деятельности в-целях обеспечения непрерывности оказания банковских услуг»
- Указание Банка России от-16.12.2021 №-6017-У про моделирование угроз-— «О-перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их-проверке и-передаче информации о-степени их-соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с-единой биометрической системой».

- Приказ Минцифры России от-07.12.2021 №-1312 «Об-утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) в-сфере электронной подписи», в-котором уменьшили число индикаторов с-4-до-3-по-сравнению с-проектом.
- Приказ Минцифры от-06.12.2021 №-1308 «Об-утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) в-сфере идентификации-и (или) аутентификации».
- Положение Банка России от-15.11.2021 №-779-П «Об-обязательных для некредитных финансовых организаций требованиях к-операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от-10-июля 2022 года №-86-ФЗ „О-Центральном банке Российской Федерации (Банке России)“, в-целях обеспечения непрерывности оказания финансовых услуг».
- Банк России принял Указание от-08.11.2021 №-5986-У «О-внесении изменений в-Указание Банка России от-8-октября 2018 года N-4927-У «О-перечне, формах и-порядке составления и-представления форм отчетности кредитных организаций в-Центральный банк Российской Федерации», которое вводит две новые формы отчетности: 0409071-— Сведения об-оценке выполнения кредитными организациями требований к-обеспечению защиты информации, 0409106-— Отчет по-управлению операционным риском в-кредитной организации.

День-2. «Культура информационной безопасности».

- Понятие культура информационной безопасности. Культура информационной безопасности как составная часть корпоративной безопасности.
- Локальные правовые акты предприятия в-области информационной безопасности. Влияние цифровой трансформации предприятия на-культуру информационной безопасности.
- Распределение зон ответственности между подразделениями предприятия по-формированию культуры информационной безопасности.
- Включение культуры информационной безопасности в-антикоррупционную политику, кодекс этики и-стандарты поведения работников предприятия.
- Доверие между работником и-работодателем как один из-принципов культуры информационной безопасности.
- Доведение требований по-информационной безопасности при приеме новых работников на-предприятии. Вводные инструктажи и-занятия.
- Требования по-информационной безопасности применимо к-различным должностям предприятия.
- Культура информационной безопасности при реализации права граждан на-обращения в-государственные инстанции.
- Мотивация персонала на-соблюдение культуры информационной безопасности.
- Отказ от-распространения слухов и-непроверенной информации как элемент культуры информационной безопасности. Защита от-манипулирования при работе с-информацией.
- Культура информационной безопасности при работе с-информацией, представленной в-электронном виде. Культура пользования техническими средствами обработки информации. Использование личных гаджетов при выполнении трудовых обязанностей.
- Культура информационной безопасности при увольнении персонала. Что можно и-что нельзя говорить после увольнения. Обеспечение конфиденциальности и-этики при прохождении собеседования с-будущими работодателями.
- Защита персональных данных работников как элемент культуры информационной безопасности.
- Защита коммерческой тайны предприятия как элемент культуры информационной безопасности.
- Методы и-приемы защиты информации при дистанционной (удаленной) работе.
- Культура информационной безопасности при работе с-открытой корпоративной информацией, доступ к-которой не-ограничен российской законодательством.
- Культура информационной безопасности при взаимоотношениях с-контрагентами. Применение политики конфиденциальности и-этики при проведении переговоров и-при выполнении условий договора.
- Культура информационной безопасности работников в-командировках, а-также на-конференциях и-иных официальных мероприятиях, проводимых другими организациями.
- Имиджевые риски при разглашении информации, компрометирующей предприятие или руководство. Противодействие черному пиару, информационным войнам и-иным неэтическим действиям со-стороны конкурентов. Основные правила информационного противоборства в-конкурентной борьбе.
- Соблюдение культуры информационной безопасности при межличностных отношениях в-трудовом коллективе, а-также при взаимоотношениях с-уволившимися работниками.
- Культура информационной безопасности в-семейных отношениях. Что можно и-что нельзя говорить родственникам. Соблюдение конфиденциальности при доведении служебной информации до-детей.
- Культура информационной безопасности и-этические нормы поведения во-внерабочее время. Размещение информации в-социальных сетях и-иных информационных ресурсах интернета.
- Культура информационной безопасности при взаимоотношениях работников с-государственными контролирующими и-правоохранительными органами.
- Проведение внутренних проверок и-расследований по-инцидентам, связанным с-нарушениями информационной безопасности на-предприятии.
- Ответственность за-нарушение требований информационной безопасности, этических норм и-стандартов поведения.

День-3. «Как организовать работу с-персональными данными в-компании: новые требования законодательства, ответственность за-несоблюдение, претензии Роскомнадзора».

Нормативно-правовое регулирование вопросов использования персональных данных.

- Система законодательных требований в-области персональных данных.
- Последние законодательные изменения.
- Персональные данные в-бизнесе: Big data, профайлинг, веб-аналитика и-обезличенные данные.

Что такое privacy compliance и-зачем он-нужен?

- Организация работы по-соблюдению законодательства о-персональных данных внутри компании.
- Функции и-задачи ответственного за-организацию обработки персональных данных (Data Protection Officer).
- Внутренний аудит в-области персональных данных.
- Бизнес-процессы с-персональными данными в-компании: основные характеристики и-типовые кейсы.
- Особенности обработки персональных данных в-электронной коммерции.

Понятие «персональные данные» и-виды персональных данных.

- Понятие «персональные данные» и-«оператор персональных данных».
- Распространение персональных данных-— новый федеральный закон №-519-ФЗ.
- Биометрические персональные данные и-специальные категории персональных данных.

Обработка персональных данных работников и-клиентов.

- Система организационно-распорядительной документации в-области персональных данных.
- Корректное определение целей и-способов обработки персональных данных.
- Правовые основания обработки персональных данных. Составление согласий в-различных ситуациях.
- Обработка персональных данных при реализации бонусных программ для клиентов.
- Порядок хранения персональных данных и-доступа к-ним. Личные дела работников.
- Порядок уничтожения персональных данных.
- Особенности работы с-персональными данными в-отделе кадров, отделе маркетинга и-других структурных подразделениях.

Обработка персональных данных в-информационных системах персональных данных (ИСПДн).

- Что такое ИСПДн?
- Система нормативных требований по-защите ИСПДн: организация их-выполнения.
- Как выполнить требование о-локализации баз персональных данных в-России (242-ФЗ)?

Трансграничная передача персональных данных.

- Требования по-трансграничной передаче и-порядок их-выполнения.
- Использование облачных и-иностранных ИСПДн на-территории России.

Уведомление об-обработке персональных данных.

- Порядок заполнения и-подачи уведомления.
- Сложности при подаче уведомления и-способы их-решения.

Сделки с-персональными данными.

- Составляем договор на-поручение обработки персональных данных: обязательные условия, хитрости, кейсы.
- Передача прав на-базы персональных данных: особенности договорного сопровождения.

Риски и-ответственность.

- Ответственность за-нарушения в-области персональных данных. Судебная практика.
- Очевидные и-неочевидные риски.
- Блокирование доступа к-интернет-сайтам.

Проверки Роскомнадзора: особенности организации и-проведения, основные выявляемые нарушения.

- Новые правила проведения контрольно-надзорных мероприятий-— Постановление Правительства от-29.06.2021 №-1046.
- Виды надзорных мероприятий. Порядок организации и-проведения плановых и-внеплановых проверок.
- Опыт сопровождения надзорных проверок: особенности подготовки к-проверке, участия в-надзорных мероприятиях, выполнения и-обжалования предписаний.

День-4. «Особенности обеспечения информационной безопасности в-органах исполнительной власти».

Критически важные структуры системы информационной безопасности федеральных органов исполнительной власти:

- СМИ.
- СМК.
- PR-структуры.

Обеспечение безопасности и-меры защиты информации в-государственных информационных системах.

- Требования к-организации защиты информации, содержащейся в-ГИС.

- Аттестация информационной системы.

Обеспечение информационной безопасности государственных данных.

- Анализ и-оценка угроз-ИБ объекта.
- Проверка защищенности объектов информатизации на-соответствие требованиям нормативных документов.

Технические средства защиты информации.

- Системы контроля и-управления доступом.
- Контролируемые каналы утечки информации.
- Особенности реализации и-интеграции с-критической информационной системой.
- Средства защиты электронной почты.

Программно-аппаратные средства обеспечения ИБ.

- Распределенные и-изолированные информационных систем.
- Методы и-протоколы авторизации.
- Безопасность удаленного доступа.
- Организация защиты ресурсов при использовании разделяемой памяти.
- Безопасность виртуальных и-облачных систем.
- Специфика угроз в-виртуальной среде.
- Угрозы, атаки при использовании облаков.

Средства обеспечения безопасности мобильных устройств специалистов государственных муниципальных учреждений.

Информационные угрозы в-социальных сетях.

- Человеческий фактор" и-социальная инженерия.
- Угрозы, связанные с-воздействием на-людей.
- «Технологические» и-«психологические» методы социальной инженерии.
- Новые угрозы, связанные с-ростом популярности социальных сетей.
- Организационные и-технические меры по-предотвращению подобных угроз.

Организация информационной защиты сайтов и-интернет-— приемных органов государственной власти.

Применение медиативных практик в-обеспечение информационных конфликтов в-публичной сфере.

День-5. «Измерение эффективности информационной безопасности».

Для чего нужно измерение эффективности ИБ?

- Можно-ли измерять ИБ?
- Зачем нужно измерять ИБ?
- Качественное и-количественное измерение?
- Все-ли измеряется деньгами или имеют-ли право на-существование нефинансовые методы измерений?
- Почему так сложно измерять ИБ? Аудитория для результатов измерений.
- Мифы об-измерении ИБ.

Метрики ИБ.

- Что такое метрики ИБ?
- Различные классификации метрик.
- KPI, PI, KRI, CSF... В-чем разница?
- База метрик.
- Где брать исходные данные для метрик.
- Как выбрать метрики?
- Метрики и-время.
- Кто выбирает метрики?
- Сколько метрик нужно?
- Тестирование метрик.
- Пересмотр метрик.
- Как презентовать метрики?

Программа управления оценкой эффективностью ИБ.

- План.
- Модель зрелости программы.
- С-чего начать?
- Ошибки при внедрении программы управления метриками
- Насколько вы-готовы к-внедрению программы?

Методы измерения ИБ.

- Оценка разрыва.
- «Сверху-вниз» и-«снизу-вверх».
- Оценка соответствия стандарту.
- Оценка по-сравнению.
- Оценка по-чек-листу.
- Оценка по-графу атак \ дереву рисков.
- Оценка рисков.
- Оценка по-опросам.
- Оценка уровня зрелости.
- Оценка по-методу «шести сигм».
- Аудит безопасности.
- Система сбалансированных показателей (BSC).
- Финансовые методы оценки.

Средства автоматизации управления метриками.

Стандарты измерения эффективности ИБ.

Прямая и-косвенная отдача от-ИБ.

Примеры проектов измерений отдельных процессов ИБ.

- Идентификация, аутентификация, авторизация и-контроль доступа.
- Повышение осведомленности, тренинги, обучение.

Примеры программ измерения-ИБ в-западных компаниях.

ПРОГРАММА ЗАОЧНОЙ ЧАСТИ.

Модуль-1. Для начинающих специалистов по-информационной безопасности.

1.1. Особенности современного цифрового информационного мира.

1.2. Тенденции.

1.3. Искусственный интеллект.

Модуль-2. Общие положения по-информационной безопасности.

2.1. Источниками конфиденциальной информации.

2.2. Составляющие информационной безопасности.

2.3. Каналы утечки конфиденциальной информации (через организацию деятельности).

2.4. Каналы утечки конфиденциальной информации (через технические средства).

2.5. Каналы утечки конфиденциальной информации (через человеческий фактор).

2.6. Меры по-защите информации.

2.7. Подготовительные мероприятия перед защитой информации.

2.8. Принципы информационной безопасности.

Модуль-3. Правовые основы информационной безопасности на-предприятии.

3.1. Информационные ресурсы в-зависимости от-доступа.

3.2. Информация в-зависимости от-порядка ее-предоставления.

3.3. Неограниченный доступ.

3.4. Конфиденциальная информация согласно Указу Президента РФ-от-06.03.1997-г. №-188-с ред.-13.07.2015.

3.5. Конфиденциальная информация согласно ФЗ-«Об-информации, информационных технологиях и-защите информации» от-27.07.2006-N 149-ФЗ (ред.-от-30.12.2021) (с-изм.-и-доп., вступ.-в-силу с-01.01.2022).

Модуль-4. Защита персональных данных.

4.1. Общее понимание терминов и-ситуации.

4.2. Отличие «распространения-ПД» и-«предоставление ПД».

4.3. «Биометрические ПД».

4.4. «Согласие» в-Федеральном законе от-27.07.2006-N 152-ФЗ (ред.-от-02.07.2021) «О-персональных данных».

4.5. «Конклюдентные действия».

4.6. «Оператор ПД».

4.7. Аутсорсинг обработки ПД. Что необходимо включить в-договор?

4.8. Подготовительные и-организационно-правовые мероприятия по-защите-ПД на-предприятии.

4.9. Технические мероприятия по-защите-ПД на-предприятии.

Модуль-5. Нормативно-правовое регулирование информационной безопасности.

5.1. Организационно-распорядительная документация по-обработке ПД.

5.2. Использование средств криптографической защиты информации (СКЗИ).

5.3. Государственный контроль за-обработкой ПД. Роскомнадзор.

5.4. Полномочия ФСТЭК России как регулятор в-области обеспечения технической защиты-ПД не-криптографическими методами.

5.5. Полномочия ФСБ России как регулятор в-области использования средств криптографической защиты информации, в-том числе для защиты ПД.

5.6. Банк России как специфического регулятора отношений в-кредитно-финансовой области.

5.7. Ответственность за-нарушение режима (разглашение) ПД, применяемая к-работнику.

5.8. Типичные нарушения операторами законодательства о-ПД (по-результатам проверок Роскомнадзора).

Модуль-6. Административная и-уголовная ответственность в-сфере информационной безопасности на-территории РФ.

6.1. Административная ответственность работодателя за-нарушение законодательства о-ПД (статья 13.11).

6.2. Административная ответственность за-разглашение информации с-ограниченным доступом (Статья-13.14-КОАП).

6.3. Уголовная ответственность за-правонарушения в-области персональных данных.

Модуль-7. Международное законодательство в-области защиты ПД.

7.1. General Data Protection Regulation (GDPR).

7.2. Принципы обработки-ПД по-GDPR.

7.3. Источники ПД.

7.4. Права субъектов ПД.

Преподаватели

ЛУКАЦКИЙ Алексей Викторович

Образование:
Окончил Московский институт радиотехники, электроники и автоматики (МИРЭА) по специальности «Прикладная математика» (специализация – «Защита информации»).

Опыт работы:

В-области информационной безопасности работает с-1992-года. Работал специалистом по-защите информации в-различных государственных и-коммерческих организациях. Прошел путь, начиная от-программиста средств шифрования и-администратора и-заканчивая аналитиком и-менеджером по-развитию бизнеса в-области информационной безопасности. Имеет ряд сертификаций в-области информационной безопасности.

Публикации:

Опубликовал свыше 600 печатных работ в-различных изданиях-— «CIO», «Директор информационной службы», «Национальный банковский журнал», «ПРАЙМ-ТАСС», «Information Security», «Cnews», «Банковские технологии», «Аналитический банковский журнал», «Business Online», «Мир связи. Connect», «Итоги», «Rational Enterprise Management», «Слияния и-поглощения» и-т.д.

РУМЯНЦЕВ Станислав Андреевич

Кандидат юридических наук, CIPP/E, старший юрист «Городисский и партнеры».

Успешно реализовал ряд compliance-проектов для международных и российских компаний и осуществляет сопровождение надзорных проверок в области персональных данных, проводимых Роскомнадзором. Специализируется на юридических аспектах внедрения информационных систем и облачных решений, электронной коммерции и разработки программного обеспечения. Представляет клиентов в судебных спорах в области персональных данных.

Прошел международную сертификацию-«Certified Information Privacy Professional/Europe» (CIPP/E).-В 2021 году назначен председателем IAPP Moscow KnowledgeNet Chapter.

Публикации:

Автор многочисленных публикаций по тематике персональных данных и права информационных технологий.-

ПАНКРАТЬЕВ Вячеслав Вячеславович

Полковник юстиции в запасе, заведующий кафедрой безопасности в Университете государственного и муниципального управления, эксперт в области корпоративной безопасности и управлению рисками, преподаватель-консультант, автор и ведущий обучающих программ (MBA, Executive MBA, открытые семинары, корпоративные мероприятия, индивидуальные консультации) по проблемам защиты бизнеса более чем в десяти учебных заведениях России.Автор книг и методических пособий по безопасности предпринимательской деятельности. Независимый консультант в области корпоративной безопасности. Разработчик методик аудита безопасности предприятия и создания КСБ – корпоративных стандартов безопасности.

Образование:

Окончил Академию ФСБ, Высшее военно-политическое училище пограничных войск КГБ СССР.

Опыт работы:

Имеет 28-тилетний опыт работы в спецслужбах КГБ, ФАПСИ, ФСО.

Корпоративные клиенты:

Среди корпоративных клиентов такие компании как: ОАО «Газпром» (корпоративный университет), ОАО «МТС» (корпоративный университет), ОАО «Мегафон», ОАО «Электрокабель», Группа компаний Armadillo, Группа компаний «Биотек», Группа компаний БТБ (Безопасные Технологии Бизнеса), Группа компаний Белагро, АФК «Система», FM Логистик, Московский залоговый банк.

Публикации:

Имеет публикации на тему защиты информации, (издательство «Арсин», данное издательство специализируется на выпуске спецлитературы). Опубликованы методические пособия «Практическое пособие по информационной безопасности предпринимательской деятельности», «Практические рекомендации по безопасности бизнеса».

ПРЕПОДАВАТЕЛЬ
Представитель Роскомнадзора.