30-я научно-техническая конференция
«Методы и технические средства обеспечения безопасности информации»
Даты проведения: 22-25 июня 2021 года

Место проведения: теплоход «Ленин»
Отправление: Санкт-Петербург, причал: «Уткина Заводь»
Октябрьская набережная, д. 31

Программа конференции МиТСОБИ 2021

22 июня, вторник

/11:30/ Встреча в зале ожидания Московского вокзала, трансфер к месту посадки на теплоход

/13:00 –14:00/ Посадка на теплоход «Ленин», размещение

/14:00 – 14:45/ Обед, ресторан «Волга»

/15:00/ Открытие конференции, конференц-зал «Ладога»

Приветствия:

Зегжда П.Д. Председатель Организационного комитета Конференции, д.т.н., проф., основатель Института кибербезопасности и защиты информации СПбПУ, Заслуженный деятель науки РФ.

Представитель Комитета по Информатизации и Связи Правительства Санкт-Петербурга

/15:30/ Круглый стол 1. Конференц-зал «Ладога»

Гибридная информационная война: стратегия победы

Доклад:

Москвин Д.А. К.т.н., доцент Института кибербезопасности и защиты информации СПбПУ

Гибридная информационная война – термин, который на слуху все последнее десятилетие. Ее не объявляют, не используют традиционное вооружение, и даже отрицают участие в ней. Целью такой войны является информационное превосходство путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственных, а результатом может стать смена руководства, изменение политического строя или даже распад страны. При этом опасным побочным эффектом такой войны в информационном поле является атмосфера тотального недоверия как между противоборствующими сторонами, так и граждан к правительствам каждой из сторон.

Как обнаружить признаки ведущейся гибридной информационной войны и есть ли надежная стратегия победы в ней? Можно ли защититься от информационных атак, не прибегая к контратакам и не развязывая гонку информационных вооружений?

Вопросы к обсуждению

1. Как отличить информационную компанию от обычных новостей?
2. Возможно ли полностью автоматизировать обнаружение fake news?
3. Можно ли безопасно пользоваться социальными сетями и сервисами, и какую информацию им можно доверить?
4. Какие психофизиологические особенности человека используются в гибридной информационной войне?
5. Как защититься от информационных кампаний?
6. Рекомендательные системы как оружие в информационной войне: как им противостоять?
7. Как гибридные информационные войны повлияют на развитие Интернета?
8. Какая стратегия участия в гибридной информационной войне наиболее эффективна?
9. Существует ли надежная стратегия защиты в гибридной информационной войне?
10. Защита или контратака: что эффективнее?

Модератор:

Зегжда Д.П. Профессор РАН, д.т.н., директор Института кибербезопасности и защиты информации СПбПУ

Эксперты:

Шеремет И.А. Д.т.н., проф., член-корр. РАН, заместитель директора РФФИ, Москва.
Баранов А.П. Д.ф-м.н., проф., заведующий кафедрой РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва
Федотов А.В. Руководитель Научно-технического центра ГРЧЦ, Москва.

/16:45/ Кофе-брейк, бар «Нева»

/17:00/ Круглый стол 2. Конференц-зал «Ладога»

Расследование киберинцидентов: выявление следов или назначение виноватых?

Доклад:

Борисов В.В. Директор по развитию ООО «НеоБИТ», Санкт-Петербург

«Русские хакеры», «вездесущее» АНБ, «армия хакеров» Китая, Кибер-ОПГ из разных стран мира – с каждой следующей кибератакой на очередной ColonialPipeline или очередную самую демократическую партию в комплекте идут заголовки, безапелляционно указывающие на нападающих. Тем не менее, расследование киберинцидентов имеет своей целью не только обнаружение виновников, но и предотвращение подобных событий в будущем. Есть ли место объективному расследованию в современном мире или потенциальные политические прибыли перевешивают возникающие риски предвзятости?

Вопросы к обсуждению

1. Процедура расследования – технические и формальные требования, что должно являться результатом?
2. Презумпция невиновности для кибератак – можно ли доказать, что вы «не верблюд»? Какие могут быть доказательства и улики?
3. Обвинять нападающих или сторону защиты? Пароли 12345test – ошибка или халатность?
4. «Все это делают» – какая деятельность в киберпространстве может являться допустимой?
5. Кто может быть действительно заинтересован в качестве расследования и нахождении истинных виновников? Кто заинтересован в политических аспектах? Договорятся ли эти две стороны?

Модератор:

Петренко С.А. Д.т.н., проф., директор по информационной безопасности, Университет Иннополис

Эксперты:

Будзко В.И. Д.т.н, проф., заместитель директора ФИЦ ИУ РАН
Жуков И.Ю. Д.т.н., проф., НИЯУ МИФИ, Заместитель генерального директора «Национальный мобильный портал», Москва

/19:00/ Торжественный ужин, посвященный открытию конференции
Ресторан «Волга»

23 июня, среда

/8:30 – 10:00/ Завтрак, ресторан «Волга»

/10:00/ Круглый стол 3. Конференц-зал «Ладога»

Санкции 2025. Время переходить на отечественное ПО?

Доклад:

Разов В.А. Научный сотрудник Института кибербезопасности и защиты информации СПбПУ

За последние несколько лет все большее количество компаний попадают под зарубежные санкции. На первый взгляд санкции – формальность, однако на деле это большие трудности с закупкой зарубежного ПО и выходом на международный рынок со своими разработками. С одной стороны, появляется все больше отечественных продуктов, которые могут заменить иностранные аналоги, с другой стороны, к ним есть много вопросов: одни сертифицированы по требованиям регуляторов, но при этом не распространяются публично; другие, находясь в открытом доступе, должным образом не протестированы на безопасность. Уже сейчас настало время определиться, какой подход является более перспективным – «обходить» санкционные ограничения или использовать только доверенное отечественное ПО? Вероятно, стоит уже сейчас обратить внимание на малоизвестные отечественные разработки, чтобы, через 3-5 лет получить протестированный доверенный безопасный продукт?

Вопросы к обсуждению:

1. Тенденция американских санкций против ИБ-сектора России – наступит ли «ИБ-апокалипсис» в России?
2. Что делать если завтра санкции введут против Вас?
3. Возможен ли успех отечественного ИБ-продукта на международной арене?
4. Путь к защищенному ПО – тематические исследования, Bug bounty или открытый исходный код?
5. Наличие ПО в «Едином реестре российских программ» – не гарантия их безопасности. Должны ли проводиться исследования ПО на безопасность при включении в реестр?

Модератор:

Коноплев А.С. К.т.н., доцент Института кибербезопасности и защиты информации СПбПУ

Эксперты:

Корт С.С. К.т.н., ведущий системный аналитик, «Лаборатория Касперского»
Макаров В.Л. Президент РУССОФТ
Будзко В.И. Д.т.н, проф., заместитель директора ФИЦ ИУ РАН

/11:30 – 12:00/ Кофе-брейк, бар «Нева»

/12:00 – 13:30/ Круглый стол 4 Конференц-зал «Ладога»

Можно ли доверять искусственному интеллекту?

Доклад 1:

Жуковский Е.В. К.т.н., доцент ИКиЗИ СПбПУ

Искусственный интеллект активно внедряется во все большее количестве программных и аппаратных продуктов, используемых в различных сферах деятельности. Зачастую на интеллектуальные системы возлагаются задачи высокой степени критичности: обеспечение безопасности, управление транспортными средствами, управление летательными средствами, анализ конфиденциальных данных, управление медицинским оборудованием. Значимость ошибки в данных сферах крайне высока. В ходе круглого стола будут рассмотрены основные аспекты обеспечения безопасности искусственного интеллекта и возникающие при этом сложности.

Проблемы безопасности систем машинного обучения

Доклад 2:

Маршалко Г.Б. Академия криптографии Российской Федерации.

Для технологий машинного обучения, как и для любой технологии, которая начинает массово внедрятся на практике, вопросы информационной безопасности пока находятся на втором плане. Однако, как и всегда, отсутствие внимания к защите приведет к серьезным инцидентам в ближайшем будущем. Уже сейчас специалистами показана возможность реализации широкого спектра атак, специфичных именно для систем машинного обучения.

Вопросы для обсуждения:

1. Какие возможны риски использования искусственного интеллекта?
2. В каких областях применение искусственного интеллекта наиболее опасно?
3. Security и safety. Функциональная безопасность систем с искусственным интеллектом: как проверить корректность работы искусственного интеллекта?
4. Возможно ли создание на основе искусственного интеллекта полностью автономного аудитора безопасности систем?
5. Моральная дилемма вагонетки: должны ли делать выбор разработчики систем ИИ или предоставлять возможность принятия решения пользователю.
6. Кто должен нести ответственность за ошибки искусственного интеллекта?

Модератор:

Иванов Д.В. К.т.н., руководитель проектов, доцент ИКиЗИ СПбПУ.

Эксперты:

Маршалко Г.Б. ТК 26, МГУ им. Ломоносова, Москва

Зегжда П.Д. Д.т.н., проф., основатель Института кибербезопасности и защиты информации СПбПУ, Заслуженный деятель науки РФ., Санкт-Петербург

/14:00 – 15:00/ Обед, ресторан «Волга»

/10:00 – 14:00/ Конференц-зал «Панорама»

Секция:

Информационная безопасность киберпространства: теория и практика

Ведущие:

Козачок А.В. Д.т.н., Академия ФСО, г. Орел.

Бирюков Д.Н. Д.т.н., проф., Заведующий кафедрой систем сбора и обработки информации ВКА им. Можайского.

1. **Хорев А.А.**
   Университет МИЭТ, Москва
   СИСТЕМА ПРАКТИКО-ОРИЕНТИРОВАННОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ (БАКАЛАВРОВ, МАГИСТРОВ) ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В НИУ МИЭТ
2. **Коваленко А.П.**
   Российский технологический университет (МИРЭА), Москва
   ОБУЧЕНИЕ МЕТОДАМ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА БАЗЕ КИБЕРПОЛИГОНА КАФЕДРЫ «ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
3. **Гуселев А.М.**
   Академия криптографии Российской Федерации, Москва
   К ВОПРОСУ О ВОЗМОЖНОСТИ ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ СХЕМ КОЛЬЦЕВОЙ ЦИФРОВОЙ ПОДПИСИ
4. **Лукин К.И.**
   ОАО «Супертел», Санкт-Петербург
   ПЕРСПЕКТИВЫ И ВОЗМОЖНОСТИ КВАНТОВОЙ КРИПТОГРАФИИ И ПРИМЕНЕНИЕ В НЕЙ ОТЕЧЕСТВЕННОЙ ЭЛЕМЕНТНОЙ БАЗЫ
5. **Правиков Д.И., Мурашкин В.А.**
   РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва
   ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ПРЕДПРИЯТИЙ ТЭК
6. **Трифаленков И.А.**
   ООО «НеоБИТ»
   ЦИФРОВОЙ ПЕРИМЕТР БЕЗОПАСНОСТИ КАК ОТВЕТ НА УГРОЗЫ СОВРЕМЕННЫМ ИНФОРМАЦИОННЫМ СИСТЕМАМ

/11:30-12:00/ Кофе-брейк, бар «Нева»

7. **Вайц В.Л.**
   Банк России, Москва
   ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИЙ ФИНАНСОВОГО СЕКТОРА: ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ
8. **Цветков А.**
   Ассоциация ФИНТЕХ, Москва
   МАСТЕРЧЕЙН – ПЕРВАЯ В РОССИИ СЕРТИФИЦИРОВАННАЯ В ФСБ ПЛАТФОРМА НА БАЗЕ БЛОКЧЕЙНА
9. **Янчук А.**
   Серчинформ, Москва
   НУЛЕВОЙ ЭТАП ЗАЩИТЫ ДАННЫХ

10. **Дрозд Ю.А.**
АО «Технологии радиоконтроля», Санкт-Петербург
ПОДХОД К БЕЗОПАСНОЙ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

11. **Киреев И.**
АО «Кросс технолоджис», Москва
ПРАКТИКА РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ КИБЕРБЕЗОПАСНОСТИ

/14:00-15:00/ Обед, ресторан «Волга»

/15:00 – 18:00/ Экскурсия в Старую Ладогу

/19:00/ Ужин, ресторан «Волга»

24 июня, четверг

/8:00 – 10:00/ Завтрак, ресторан «Волга»

/10:00 – 11:30/ Круглый стол 5. Конференц-зал «Ладога»

Тестирование на проникновение: искусство или формальность

Доклад:

Орел Е.М. Научный сотрудник Института кибербезопасности и защиты информации СПбПУ

Защищенность IT-инфраструктуры является одним из важнейших требований, предъявляемых к организациям всех возможных отраслей, лишь недавно получившим нормативную поддержку. В рамках круглого стола будут проанализированы существующие методики оценки защищенности IT-инфраструктуры. Будут рассмотрены подходы к организации тестирования на проникновение, возможности его автоматизации, а также мировой опыт нормативного регулирования в области тестирования на проникновение.

Вопросы к обсуждению:

1. Как оценить качество проведенного тестирования?
2. Нужна ли жесткая формализация процесса тестирования на проникновение?
3. Когда нужно остановить пентест?
4. Возможна ли полная автоматизация пентеста?
5. Этические проблемы тестирования на проникновение.

Модератор:

Москвин Д.А. К.т.н., доцент Института кибербезопасности и защиты информации СПбПУ

Эксперты:

Рудина Е.А. К.т.н., старший системный аналитик, «Лаборатория Касперского»

Жуков И.Ю. Д.т.н., проф., НИЯУ МИФИ, Заместитель генерального директора «Национальный мобильный портал»

/11:30-12:00/ Кофе-брейк, бар «Нева»

/12:00 – 13:30/ Круглый стол 6, Конференц-зал «Ладога»

Утечки персональных данных: как контролировать свои данные в сети?

Доклад:

Дахнович А.Д. Научный сотрудник Института кибербезопасности и защиты информации СПбПУ

Практически каждый день в новостях появляются заголовки «В сеть утекла база данных…». Браузеры уведомляют пользователей об «утекших в сеть» паролях и в каких ресурсах потенциально аккаунты могут быть взломаны. Некоторые пользователи используют «менеджеры паролей» с хранением сложных, сгенерированных паролей или используют одноразовые пароли для входа. Но и их периодически взламывают. Данные факты свидетельствуют о том, что необходимо менять отношение к информации, которую мы оставляем в сети. В последнее время не только социальные сети, но и практически каждый Интернет-магазин хранит и использует персональные данные, интересы, профиль поведения. Пользователи физически не могут контролировать и запоминать все сайты и сервисы, на которых они оставляли информацию о себе.
В рамках круглого стола попробуем разобраться, можно ли сломать тенденцию и остановить нарастающую лавину утечек данных со всевозможных Интернет-сервисов, или мы должны адаптироваться и научиться жить в условиях полной открытости.

Вопросы к обсуждению:

1. Анонимность и цифровая чистота: неразрывны ли эти понятия?
2. Можно ли превентивно защитить персональные данные или мы всегда будем бороться с последствиями утечек?
3. Можно ли контролировать распространение своих персональных данных? Какие средства предотвращения от утечек уже доступны сегодня?
4. Трансграничность Интернета: поможет ли перенос всех персональных данных граждан в пределы государства от их утечек?
5. Будущее персональных данных: грозит ли нам потеря приватности данных?

Модератор:

Павленко Е.Ю. К.т.н., руководитель проектов.

Эксперты:

Федотов А.В. Руководитель Научно-технического центра ГРЧЦ, Москва.
Баранов А.П. Д.ф-м.н., проф., заведующий кафедрой РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва
Лукин К.И. Генеральный директор АО «Супертел»

/10:00 – 14:00/ Конференц-зал «Панорама»

Секция:

Информационная безопасность: взгляд молодых ученых

Ведущие:

Иванов Д.В. К.т.н., руководитель проектов.
Платонов В.В. К.т.н., доцент ИКиЗИ СПбПУ

1. **Сабиров Э.**
(МГУ им. Ломоносова), Маршалко Г.Б. (АК РФ)
ЗАЩИТА ПРИВАТНОСТИ ИЗОБРАЖЕНИЙ ПРИ ИХ ПУБЛИКАЦИИ

2. **Завадский Е.В., Иванов Д.В.**
Санкт-Петербургский политехнический университет Петра Великого
СОЗДАНИЕ ВИРТУАЛЬНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ РАЗЛИЧНОЙ ОТРАСЛЕВОЙ ПРИНАДЛЕЖНОСТИ И ПРОИЗВОЛЬНОГО МАСШТАБА В УСЛОВИЯХ ОГРАНИЧЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ

3. **Фатин А.Д., Павленко Е.Ю.**
Санкт-Петербургский политехнический университет Петра Великого
ОБЕСПЕЧЕНИЕ КИБЕРУСТОЙЧИВОСТИ СИСТЕМ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОЭВОЛЮЦИОННЫХ АЛГОРИТМОВ

4. **Кубрин Г.С., Иванов Д.В., Зегжда Д.П.**
Санкт-Петербургский политехнический университет Петра Великого
ПРИМЕНЕНИЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ И ГРАФОВОГО ПРЕДСТАВЛЕНИЯ БАЙТ-КОДА ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ

/11:30 – 12:00/ Кофе-брейк, бар «Нева»

5. **Синцова К.А.**
НИУ ВШЭ, Санкт-Петербург
ИССЛЕДОВАНИЕ АКТУАЛЬНЫХ МАТЕМАТИЧЕСКИХ ФОРМАЛИЗАЦИЙ В ВОПРОСАХ МОДЕЛИРОВАНИЯ КС

6. **Зубков Е.А., Жуковский Е.В., Зегжда Д.П.**
Санкт-Петербургский политехнический университет Петра Великого
ОЦЕНКА ЗАЩИЩЕННОСТИ ГЕТЕРОГЕННЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ АНАЛИЗА СЕТЕВОЙ ТОПОЛОГИИ

7. **Гулин Н.А.**
Санкт-Петербургский политехнический университет Петра Великого
ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ОТРИЦАЕМОГО ШИФРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

8. **Огнев Р. А., Жуковский Е.В.**
Санкт-Петербургский политехнический университет Петра Великого
ПОВЫШЕНИЕ СВЯЗНОСТИ ГРАФОВОГО ПРЕДСТАВЛЕНИЯ ПРОГРАММЫ НА ОСНОВЕ АНАЛИЗА НЕПРЯМЫХ ПЕРЕХОДОВ ДЛЯ ОБНАРУЖЕНИЯ НЕБЕЗОПАСНЫХ ФУНКЦИЙ

/14:00-15:00/ Обед, ресторан «Волга»

/15:00 – 18:00/ Экскурсия на о. Валаам

/19:00/ Ужин, ресторан «Волга»

Закрытие конференции

25 июня, пятница

Завтрак, ресторан «Волга» /8:30 – 10:00/

Прибытие в г. Санкт – Петербург /10:00/

NeoQUEST

Соревнование по кибербезопасности

Место проведения: пространство KOD
ул. Комсомола д. 2

На протяжении всего дня, с 11:00 до 18:00, можно принять участие в онлайн-конкурсах:

Квест «ЕГЭ по ИБ»

/11:00 – 13:30/ Зал № 1. Доклады

Владимир Разов: «Как без железа хакнуть железо»

Максим Башканков: «Как тебе такое, Google Play? Находим ранее не обнаруженные вирусы под андроид»

Секция FAST TRACK

Владислав Данилов: «Поиск уязвимостей в 1 клик. Миф или реальность?!»

Евгений Зубков: «Строим виртуальные сети: для работы и обучения»

Александр Чагочкин: «Атаки на системы распознавания лиц»

/13:30 – 14:00/ Кофе-брейк

Алексей Бусыгин: «Обходим UEFI Secure Boot для компрометации полного шифрования диска в Linux»

Григорий Пагуба: «Королевская битва: выбираем лучший бесплатный декомпилятор для статического анализа руткитов»

Никита Гололобов: «Электрический ARMармагеддон (Обход Trustzone-M с использованием fault-injection)»

Людмила Осипова: «Код с кэшбеком: читаем данные из памяти»

/16:30 – 17:00/ Кофе-брейк

ВОРКШОПЫ

Зал № 2

/11:00 – 13:30/ Полина Аверьянова, Анна Штыркина

/14:00 – 16:30/ Максим Вотчеников

/17:00 – 18:00/ Подведение итогов квеста «ЕГЭ по ИБ»
Подведение итогов финала HackQuest
Награждение победителей

Учредители и организаторы

Комитет по науке и высшей школе Санкт-Петербурга

191060, Центральный район, Смольный
Телефоны: (812) 576-71-60
Факс: (812) 576-77-04
knvsh@gov.spb.ru
http://www.gov.spb.ru/gov/admin/otrasl/c_science

Предметами ведения Комитета по науке и высшей школе являются:

1. Определение и осуществление политики в области среднего, высшего, послевузовского профессионального образования и дополнительного образования, науки, инновационной деятельности в области науки и высшего профессионального образования, не противоречащей политике Российской Федерации в области образования и науки.
2. Формирование и реализация программ развития системы среднего, высшего, послевузовского профессионального образования и дополнительного образования, с учетом потребностей среднесрочных и долгосрочных приоритетов социально-экономического развития Санкт-Петербурга.
3. Управление и координация научно-исследовательской и образовательной деятельности учреждений среднего, высшего и дополнительного профессионального образования, разработка и реализация научных программ и проектов, осуществляемых в интересах Санкт-Петербурга.
4. Иные задачи в сфере образования в соответствии с законодательством Российской Федерации и Санкт-Петербурга.
Более подробную информацию о Комитете можно найти по адресу:
http://www.gov.spb.ru/gov/admin/otrasl/c_science/subject

Комитет по информатизации и связи Санкт-Петербурга

Смольный, Санкт-Петербург, 191060
Телефон: (812) 576-7123
Факс: (812) 576-7345
kis@gov.spb.ru
http://www.gov.spb.ru/gov/admin/otrasl/c_information

Комитет по информатизации и является исполнительным органом государственной власти Санкт-Петербурга.

Комитет проводит государственную политику Санкт-Петербурга в сфере информатизации и связи, управления информационными и телекоммуникационными ресурсами Санкт-Петербурга, обеспечения информационной безопасности и защиты информации, содержащей сведения государственной или служебной тайны, в исполнительных органах государственной власти Санкт-Петербурга, а также координирует деятельность исполнительных органов государственной власти Санкт-Петербурга в данной сфере.
Комитет в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, иными нормативными правовыми актами Российской Федерации, Уставом Санкт-Петербурга, законами Санкт-Петербурга, иными нормативными правовыми актами Санкт-Петербурга, постановлениями и распоряжениями Губернатора Санкт-Петербурга, постановлениями и распоряжениями Правительства Санкт-Петербурга, а также

настоящим Положением.

Комитет осуществляет обеспечение деятельности Научного совета по информатизации Санкт-Петербурга, Комиссии по защите информации в исполнительных органах государственной власти Санкт-Петербурга, Экспертно-координационного совета Санкт-Петербурга в области связи и телекоммуникаций.

Основными задачами Комитета являются:

- Реализация государственной политики Санкт-Петербурга в сфере информатизации, связи и защиты информации.
- Координация деятельности исполнительных органов государственной власти Санкт-Петербурга в сфере информатизации, связи и защиты информации.
- Организация защиты государственных информационных ресурсов от несанкционированного доступа, копирования и разрушения, а также обеспечение безопасности информационных и телекоммуникационных систем и сетей исполнительных органов государственной власти Санкт-Петербурга.
- Осуществление других задач в сфере информатизации, телекоммуникаций и связи, защиты информации в соответствии с действующим законодательством.

Более подробную информацию о Комитете можно найти по адресу:
http://www.gov.spb.ru/gov/admin/otrasl/c_information

Федеральный исследовательский центр Информатика и Управление Российской академии наук

Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН)

Адрес: 119333, г. Москва, ул.Вавилова, д. 44, корп. 2
www.ipiran.ru

Институт проблем информатики Российской академии наук (ИПИ РАН) образован в 1983 г.
Институт входит в состав Отделения нанотехнологий и информационных технологий Российской академии наук.
ИПИ РАН выполняет фундаментальные, прикладные исследования и разработки в области построения интегрированных информационно-телекоммуникационных сетей и систем, стохастических систем, в области накопления, обработки и отображения информации (текста, видео, аудио), создания информационно-вычислительных систем новых поколений.
Институт проблем информатики Российской академии наук является учредителем и издателем научного журнала «Информатика и её применения».

СЗРО УМО по ИБ при СПбПУ ПОЛИТЕХ

СЗРО УМО

Санкт-Петербург, ул. Политехническая д. 29, ауд. 173.
http://ibks.ftk.spbstu.ru/szro-umo/

Северо-Западное региональное отделение учебно-методического объединения по образованию в области информационной безопасности (СЗРО УМО) создано на базе ФГБОУ ВПО «СПбГПУ» на основании решения Пленума Учебно-методического объединения по информационной безопасности при Институте криптографии, связи и информатики Академии ФСБ РФ от 28 июля 2012 года.
СЗРО УМО объединяет кафедры осуществляющие подготовку в области информационной безопасности 12 ВУЗов Северо-Запада. СЗРО УМО в области информационной безопасности является государственно-общественной организацией в системе высшего профессионального образования Россий-

ской Федерации.

Основными задачами СЗРО УМО являются:

координация действий научно-педагогической общественности кафедр вузов Северо-Запада России, в обеспечении качества и развития содержания высшего профессионального образования в области информационной безопасности;

участие в разработке проектов государственных образовательных стандартов, примерных основных образовательных программ, другой учебно-программной документации;

экспертиза учебно-методической документации, необходимой для обеспечения подготовки специалистов в области информационной безопасности.

Наряду с выполнением основных задач СЗРО УМО принимает участие в работе Координационного совета УМО по информационной безопасности при Институте криптографии, связи и информатики Академии ФСБ РФ, выполнении научно-исследовательских работ в области развития методов и средств по защите информации, методики преподавания, лицензировании образовательной деятельности вузов, грифовании учебной и методической литературы, научно-методическом сопровождении образовательной деятельности кафедр.

Деятельность УМО «СПбГПУ» осуществляется на основе Положения о СЗРО УМО, разработанного на базе Положения об Учебно-методическом объединении по информационной безопасности при Институте криптографии, связи и информатики Академии ФСБ РФ.

МОО «Ассоциация защиты информации»
125438, Москва, 4-й Лихачевский пер., д.15, МОО «АЗИ»
Телефон/факс: +7 (499) 154-61-55
azi@azi.ru
http://azi.ru/

Межрегиональная общественная организация «Ассоциация защиты информации» (АЗИ) образована в 2002 году по инициативе ФАПСИ и Гостехкомиссии России. Деятельность АЗИ направлена на создание благоприятных условий для реализации потребностей граждан, бизнеса и органов государственной власти в продуктах и технологиях защиты информации.

АЗИ активно взаимодействует с аппаратом Совета Безопасности РФ, ФСБ России, Федеральной службой технического и экспортного контроля (ФСТЭК), Федеральным агентством по информационным технологиям (ФАИТ), другими министерствами и ведомствами, а также со многими финансово-экономическими структурами.

Устав АЗИ дает право осуществлять международные связи, разрешает вступать в международные общественные объединения, а также осуществлять внешнеэкономическую деятельность.

АЗИ является лицензиатом ФСБ России и Гостехкомиссии России, что дает ей право:

- осуществлять мероприятия и оказывать услуги по технической защите конфиденциальной информации;
- вести деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- осуществлять работы, связанные с использованием сведений, составляющих государственную тайну;
- вести разработку, производство, осуществлять техническое обслуживание и распространение шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Ассоциация готова оказывать содействие в налаживании деловых контактов и связей с целью реализации продуктов и технологий защиты информации, обмена деловой информацией, осуществления совместных разработок и промышленного производства, проведения симпозиумов, конференций, выставок, семинаров, организации обучения специалистов в области информационной безопасности.

Предприятия, представленные в Ассоциации, предоставляют полный комплекс услуг по созданию и сопровождению интегрированных комплексных систем безопасности. Работы выполняются как с предпроектного этапа, так и на любом этапе создания и реконструкции объектов.

Генеральный спонсор конференции
ООО «НеоБИТ»

195220, Россия, г.Санкт-Петербург, ул.Гжатская, д.21 «Г»
Телефоны: (812) 535-28-06; 535-88-67; 535-88-84
Факс: (812) 535-29-41
info@neo-bit.ru
http://www.neo-bit.ru/
www.необит.рф

Компания ООО «НеоБИТ» создана командой ведущих специалистов в области информационной безопасности для продвижения на российский и мировой рынок решений и передовых технологий, разрабатываемых российскими учеными, отечественных продуктов и решений, направленных на обеспечение защиты информационных систем.
В компании работают доктора технических наук, кандидаты технических наук, ведущие специалисты высшей квалификации в области защиты информации, создания телекоммуникационных систем и систем связи. Профессионализм наших сотрудников подтвержден опытом реализации проектов различного масштаба, многочисленными дипломами и сертификатами.
Профиль компании – проектирование и разработка продуктов и решений, обеспечивающих безопасность информации, создание защищенных информационных систем.
Компания «НеоБИТ» активно сотрудничает с академическими и образовательными институтами регионального и федерального уровня, является партнером Специализированного Центра Защиты Информации (Санкт-Петербург).

Партнеры конференции

Санкт-Петербургский информационно-аналитический центр

191040, Санкт-Петербург, ул.Черняховского, д.59
Телефон: (812) 764-39-57
Факс: (812) 764-95-48
secretar@iac.spb.ru
http://www.iac.spb.ru/about/

Санкт-Петербургский информационно-аналитический центр (СПб ИАЦ) — государственное унитарное предприятие, работающее в области информатизации и информационного обеспечения органов государственной власти Санкт-Петербурга и других организаций, а также предоставления услуг в сфере создания и использования современных информационных и телекоммуникационных систем, средств и технологий.
СПб ИАЦ находится в ведении Комитета по информатизации и связи Санкт-Петербурга.
В компетенции СПб ИАЦ — разработка и реализация информационных и информационно-аналитических проектов и систем в различных предметных областях.
Экспертиза СПб ИАЦ базируется на многолетнем опыте успешной работы в сфере информатизации органов государственной власти и ряде проектов для государственных и коммерческих компаний.
Основными задачами СПб ИАЦ являются создание, сопровождение и системная интеграция информационных и информационно-аналитических систем Администрации Санкт-Петербурга и подведомственных ей организаций на основе современных достижений информационных и телекоммуникационных технологий.

Основные направления деятельности:

- Разработка информационно-аналитических и информационных систем в разных предметных областях,
- Эксплуатация информационно-аналитических и информационных систем в разных предметных областях.
- Основная цель – оказание услуг, удовлетворяющих и превосходящих по своему качеству ожидания потребителей, соответствующих стандарту ISO 9001:2008, получение устойчивой прибыли для дальнейшего развития предприятия в интересах наших потребителей, сотрудников и других заинтересованных сторон.

НП «РУССОФТ»

199034, Санкт-Петербург, Биржевая линия,
д. 16, оф. 411
Телефон: +7 (812) 457-15-47
Факс: +7 (812) 457-15-47
info@russoft.org
https://russoft.org/contacts/

РУССОФТ является наиболее влиятельным объединением компаний-разработчиков программного обеспечения России. Мы объединяем 234 ИТ-компании со штатом более 70 000 высококвалифицированных сотрудников. РУССОФТ представляет всю индустрию разработки ПО в России. Центральный офис Партнерства находится в Санкт-Петербурге. Мы предоставляем ИТ-компаниям новые возможности для выхода на глобальный рынок.

СПб филиал ОАО «НПК «ТРИСТАН»

195220, г.Санкт-Петербург, пр.Непокоренных, д.47
Телефон: (812) 535-2246
Факс: (812) 535-2716
М.т.: +7(911) 911-40-55, +7(901) 970-74-57
spb-tristan@mail.ru

Компания ОАО «НПК «Тристан» возникла в 2002 году в Москве как разработчик аппаратуры цифровой обработки сигналов и специализируется на создании сверхнадежных радиоэлектронных средств и сложных радиотехнических радиолокационных систем. ОАО «НПК «Тристан» является главным исполнителем научно-технической программы союзного государства России и Беларуси – «Траектория». Сегодня в компании работает около 200 человек, большая часть из которых занята разработками как оборудования, так и программных продуктов.

ФГУП «НИИ «КВАНТ»

125438 г.Москва, 4-й Лихачевский пер., д.15
Телефон: (499) 745-73-02
info@rdi-kvant.ru
http://www.rdi-kvant.ru/

ФГУП «НИИ «Квант» является коммерческим юридическим лицом, созданным для удовлетворения государственных и общественных потребностей в области создания специальных технических и программных средств.

Основными видами деятельности института являются:

- проведение фундаментальных, поисковых и прикладных научных исследований, научно-исследовательских и опытно-конструкторских работ в области создания электронно-вычислительной техники, техники связи и телекоммуникаций, систем и средств обработки данных и изделий радиоэлектронной и вычислительной техники;
- разработка, производство, реализация, ремонт, гарантийное и послегарантийное обслуживание электронно-вычислительных средств и комплексов специального и гражданского назначения, в том числе содержащих драгоценные металлы;
- исследование и прогнозирование развития специальных технических средств связи;
- внешнеэкономическая деятельность;
- проведение работ, связанных с созданием средств защиты информации;
- разработка, производство, реализация и приобретение в целях продажи СВТ и систем;
- разработка, производство, реализация и ремонт электронных изделий гражданского назначения, товаров народного потребления;
- выполнение экоаналитических работ по аккредитованным направлениям, в том числе проведение производственного контроля за состоянием окружающей среды и получение базовой экоаналитической информации;
- разработка, аттестация и сертификация испытательного оборудования и средств измерений, поверка, калибровка и ремонт измерительной аппаратуры;
- оказание научных, технических, проектно-конструкторских, вычислительных, информационных, консультационных услуг.
- Безопасное проектирование и защита приложений
- Защита веб-приложений и мобильных приложений без ограничения бизнес-операций
- Консалтинговые услуги в области анализа и обеспечения безопасности (US)
- Развертывание функций защиты в масштабе всех ИТ-сред