27-я научно-техническая конференция
«Методы и технические средства обеспечения безопасности информации»
Даты проведения: 24-27 сентября 2018 года

Место проведения: г. Санкт-Петербург, Крестовский остров, ул. Рюхина 9а,
отель «Parklane Resort and Spa»

Программа конференции МиТСОБИ 2018

24 сентября, понедельник

Встреча приезжающих на Московском вокзале в зале ожидания у памятника Петру I. Трансфер в отель «Parklane» /11:00 – 11:30/

Регистрация и размещение участников конференции в отеле /12:30 – 13:00/

Обед ресторан «Атриум» /13:00 – 14:00/

Пленарное заседание /14:00/

Приветствия:

— **Представитель Комитета по Информатизации и Связи Правительства Санкт-Петербурга**
— **Зегжда П.Д.** Председатель Организационного комитета Конференции, д.т.н., проф., руководитель отделения «Кибербезопасность» СПбПУ, Заслуженный деятель науки РФ.
— **Лютиков В.С.** к.т.н., Заместитель Директора, ФСТЭК
— **Лось В.П.** МОО АЗИ, д.в.н., проф. заведующий кафедрой МИРЭА, Лауреат премии Правительства РФ в области образования

Пленарные доклады:

Соколов И.А.
д.ф-м.н., проф., Академик РАН Директор ФИЦ ИУ РАН
Некоторые проблемы информационной безопасности

Баранов А.П.
д.ф-м.н., проф., Заместитель Генерального директора АО ГНИВЦ
Проблемы удаленной аутентификации

Смирнов А.И.
д.и.н., проф., генеральный директор Национальной ассоциации ИБ; Президент НИИГЛОБ; Главный научный сотрудник МГИМО
Глобальная безопасность в эпоху гибридных войн: информационный кейс

Перерыв /15:30 – 15:45/

Круглый стол 1 /15:45 – 16:45/

«Кибербезопасность и цифровизация производства. Возможен ли компромисс?»

Спикер: Коноплев А.С., к.т.н., заместитель генерального директора ООО «НеоБИТ»

Модератор: Зегжда Д.П., профессор РАН, д.т.н., Заведующий кафедрой ИБКС СПбПУ

Эксперты:

Соколов И.А.
Д.ф-м.н., проф., Академик РАН, Директор ФИЦ ИУ РАН

Баранов А.П.
Д.ф-м.н., проф., Заместитель Генерального директора АО ГНИВЦ

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

Лютиков В.С.
К.т.н., Заместитель директора, ФСТЭК

Зегжда П.Д.
Д.т.н., проф., руководитель отделения «Кибербезопасность» СПбПУ, Заслуженный деятель науки РФ

Латышев Д.Л.
Начальник отдела защиты информации. Центр компетенций по ИБ АСУ ТП ПАО «Газпром нефть»

Духвалов А.П.
Руководитель управления перспективных технологий, «Лаборатория Касперского»

Вопросы для обсуждения:

1. Какие новые угрозы безопасности возникают в процессе цифровизации производства?
2. Проблемы нормативного регулирования. Кто и как определит, безопасно ли цифровое производство?
3. Конфиденциальность, целостность, доступность. Трансформируется ли понятие «безопасность» при переходе предприятия на цифровой формат?
4. Какие существуют альтернативные стратегии и механизмы обеспечения безопасности в системах цифрового производства?
5. Безопасность или высокий уровень цифровизации производства. Как добиться компромисса?

Кофе-брейк /16:45 – 17:15/

Круглый стол 2 /17:15 – 18:30/

«Приватность личного пространства в цифровом мире»

Спикер: Москвин Д.А. к.т.н., технический директор ООО «НеоБИТ»

Модератор: Петренко С.А. д.т.н., проф., директор по информационной безопасности, Университет Иннополис

Эксперты:

Соколов И.А.
Д.ф-м.н., проф., Академик РАН, Директор ФИЦ ИУ РАН

Баранов А.П.
Д.ф-м.н., проф., Заместитель Генерального директора АО ГНИВЦ

Смирнов А.И.
Д.и.н., проф., генеральный директор Национальной ассоциации ИБ; Президент НИИГЛОБ; Главный научный сотрудник МГИМО

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

Качалин А.И.
К.т.н., Исполнительный директор Центра Киберзащиты, Сбербанк.

Вопросы для обсуждения:

1. Готовы ли мы платить личными данными за «бесплатные» сервисы?
2. Запрет криптографии в мессенджерах: необходимость для безопасности государства и борьбы с терроризмом?
3. Зачем люди все сами рассказали о себе в соцсетях?
4. Можно ли обеспечить приватность информации о людях в цифровом мире в условиях, когда человек неотличим от бота?
5. Защита личности в цифровом мире. Технологические аспекты.

Подведение итогов круглых столов. Выступление модераторов.

Зал «Крестовский»: демонстрационный стенд

«Интеллектуальное управление безопасностью умного транспорта»

Торжественный банкет в честь открытия конференции /19:00/
Ресторан «Parklane»

25 сентября, вторник

Завтрак /8:30 – 10:00/ ресторан «Атриум»

Секция 1. Зал «Крестовский 1»
/10:00 – 13:00/

Исследование и оценка безопасности распределенных информационных систем на основе современных интеллектуальных технологий (Big Data, нейросетевые методы, машинное обучение)

Руководители заседания:

Зегжда П.Д. *Д.т.н., проф., руководитель отделения «Кибербезопасность» СПбПУ*

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

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

---

1. **Полтавцева М.А.**
   Санкт-Петербургский политехнический университет Петра Великого.
   ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ.

2. **Саенко И.Б., Чечулин А.А., Виткова Л.А.**
   СПИИРАН, Санкт-Петербург
   КОНЦЕПЦИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ АНАЛИТИЧЕСКОЙ ОБРАБОТКИ ЦИФРОВОГО СЕТЕВОГО КОНТЕНТА С ЦЕЛЬЮ ОБНАРУЖЕНИЯ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ.

3. **Данилов В.В.**
   Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
   МОДЕЛЬ ОЦЕНИВАНИЯ ЗНАЧЕНИЙ ВРЕМЕННЫХ ХАРАКТЕРИСТИК СЕТЕВОГО ТРАФИКА СЕРВИСОВ ДОМЕННЫХ ИМЕН В ЗАДАЧАХ ПРОФИЛИРОВАНИЯ СУБЪЕКТНО-ОБЪЕКТНОГО ВЗАИМОДЕЙСТВИЯ.

4. **Семенов В.В., Сухопаров М.Е., Лебедев И.С.**
   ИТМО, АО «НПК Тристан», СПИИРАН
   МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕМЕНТОВ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ.

Кофе-брейк /11:15 – 11:30/

5. **Падарян В.А.**
   ИСП РАН, г. Москва.
   МЕТОДЫ И СРЕДСТВА АНАЛИЗА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ В УСЛОВИЯХ ОТСУТСТВИЯ ИСХОДНОГО КОДА.

6. **Афонин Д.Г.**
   Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
   ПОДХОД К ВОССТАНОВЛЕНИЮ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММ, ИСПОЛЬЗУЮЩИХ ЗАРАНЕЕ ПОДГОТОВЛЕННЫЕ АТАКУЮЩИЕ ФРАГМЕНТЫ КОДА.

7. **Штыркина А.А, Зегжда П.Д., Лаврова Д.С.**
   Санкт-Петербургский политехнический университет Петра Великого.
   ОБНАРУЖЕНИЕ АНОМАЛИЙ В ТРАФИКЕ МАГИСТРАЛЬНЫХ СЕТЕЙ ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ МУЛЬТИФРАКТАЛЬНОГО АНАЛИЗА.

8. **Алексеев И.В., Зегжда П. Д., Лаврова Д.С., Штыркина А.А.**
   Санкт-Петербургский политехнический университет Петра Великого.
   АНАЛИЗ БЕЗОПАСНОСТИ МАГИСТРАЛЬНЫХ КАНАЛОВ СВЯЗИ НА ОСНОВЕ КОНТРОЛЯ ЗАВИСИМОСТЕЙ ПАРАМЕТРОВ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ.

Обед /13:00 – 14:00/ ресторан «Атриум»

Секция 1, продолжение. Зал «Крестовский 1»

/14:00 – 18:00/

Исследование и оценка безопасности распределенных информационных систем на основе современных интеллектуальных технологий (Big Data, нейросетевые методы, машинное обучение)

Руководители заседания:

Зегжда П.Д. *Д.т.н., проф., руководитель отделения «Кибербезопасность» СПбПУ*

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

Трифаленков И.А. *К.т.н. руководитель направления, Huawei в России*

---

9. **Платонов В.В., Семенов П.О.**
   Санкт-Петербургский политехнический университет Петра Великого.
   ПОДХОДЫ К ОБНАРУЖЕНИЮ АТАК В СЕТЯХ VANET.

10. **Крундышев В.М., Демидов Р.А., Зегжда П.Д., Калинин М.О.**
    Санкт-Петербургский политехнический университет Петра Великого.
    СОВРЕМЕННЫЕ НЕЙРОСЕТЕВЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ КИБЕРУГРОЗ, НАПРАВЛЕННЫХ НА ДИНАМИЧЕСКИЕ СЕТЕВЫЕ ИНФРАСТРУКТУРЫ БЕСПИЛОТНОГО ТРАНСПОРТА.

11. **Крюков Р.О., Зима В.М.**
    Военно-космическая академия имени А. Ф. Можайского. Санкт-Петербург.
    АНАЛИЗ УЯЗВИМОСТЕЙ СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ ГИБРИДНОГО ТЕСТИРОВАНИЯ.

12. **Овасапян Т.Д., Москвин Д.А., Иванов Д.В.**
    Санкт-Петербургский политехнический университет Петра Великого.
    ИСПОЛЬЗОВАНИЕ АППАРАТА НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ ВНУТРЕННИХ НАРУШИТЕЛЕЙ В VANET-СЕТЯХ.

Кофе-брейк /15:45 – 16:15/

13. **Зайцева Е.А., Платонов В.В.**
Санкт-Петербургский политехнический университет Петра Великого.
ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ МУРАВЬИНОГО АЛГОРИТМА.

14. **Малышев Е.В., Москвин. Д.А.**
Санкт-Петербургский политехнический университет Петра великого.
ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ VANET-СЕТЕЙ.

15. **Романов П.А.**
Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
ТЕХНОЛОГИЯ ДИАГНОСТИРОВАНИЯ ПРИЗНАКОВ И ПАРАМЕТРОВ УЯЗВИМЫХ СОСТОЯНИЙ СЕТЕВЫХ УЗЛОВ В ЗАДАЧАХ УДАЛЁННОГО СЕТЕВОГО МОНИТОРИНГА.

16. **Саенко И.Б., Кушнеревич А.Г., Браницкий А.А.**
СПИИРАН, Санкт-Петербург.
ПОДХОД К ОБНАРУЖЕНИЮ АТАК НА УСТРОЙСТВА ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ РАСПРЕДЕЛЕННОЙ ОБРАБОТКИ ДАННЫХ И ИСПОЛЬЗОВАНИЯ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ.

Секция 2. Зал «Крестовский 2»
/10:00 – 13:00/

Информационная безопасность: взгляд молодых ученых

Руководители заседания:

Бирюков Д.Н. *Д.т.н., проф., Военно-космическая академия имени А. Ф. Можайского.*
Платонов В.В. *К.т.н., Санкт-Петербургский политехнический университет Петра Великого.*
Москвин Д.А. *К.т.н. технический директор ООО «НеоБИТ».*

---

1. **Васильев Д.О., Магомедов Ш.Г.**
Российский технологический университет МИРЭА.
ФОРМИРОВАНИЕ СОСТАВА СРЕДСТВ ПРОТИВОДЕЙСТВИЯ В СИСТЕМАХ РАЗГРАНИЧЕНИЯ И КОНТРОЛЯ ДОСТУПА.

2. **Визавитин О.И., Ершов Н.С., Журавлев С.И.**
Российский технологический университет МИРЭА.
СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО НЕЗАЩИЩЕННЫМ СОЕДИНЕНИЯМ.

3. **Гаранин А.В., Сикарев И.А.**
ГУМРФ им. адм. С.О. Макарова
ПОВЫШЕНИЕ ЭЛЕКТРОМАГНИТНОЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ КАНАЛОВ МОНИТОРИНГА БЕЗЭКИПАЖНЫХ СУДОВ С ИСПОЛЬЗОВАНИЕМ СЛОЖНЫХ ПАРАЛЛЕЛЬНЫХ СИГНАЛОВ.

4. **Самолетова К.С.**
   Российский технологический университет МИРЭА,
   Карпов И.А.
   Высшая школа экономики, Москва.
   ПРИМЕНЕНИЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ В ЗАДАЧЕ ВЫЯВЛЕНИЯ ОРГАНИЗОВАННЫХ ИНФОРМАЦИОННЫХ КАМПАНИЙ.

5. **Никифорова Л.О.**
   Московский государственный университет им. М.В. Ломоносова, г. Москва,
   Маршалко Г.Б.
   Технический комитет по стандартизации ТК 26, г. Москва.
   СПУФИНГ АТАКА НА БИОМЕТРИЧЕСКУЮ СИСТЕМУ ИДЕНТИФИКАЦИИ, ИСПОЛЬЗУЮЩУЮ АЛГОРИТМ РАСПОЗНАВАНИЯ EIGENFACES.

6. **Круглова С.И.**
   Московский государственный университет им. М.В. Ломоносова, г. Москва,
   Маршалко Г.Б.
   Технический комитет по стандартизации ТК 26, г. Москва.
   ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ОБХОДА БИОМЕТРИЧЕСКИХ СИСТЕМ ИДЕНТИФИКАЦИИ ПО ЛИЦАМ, ИСПОЛЬЗУЮЩИХ АЛГОРИТМ LBP.

Кофе-брейк /11:30 – 11:45/

7. **Васильева К.В., Коноплев А.С.**
   Санкт-Петербургский политехнический университет Петра Великого.
   АНАЛИЗ ВСТРОЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ UEFI BIOS НА ПРЕДМЕТ НАЛИЧИЯ НДВ.

8. **Жуковский Е.В., Зегжда Д.П.**
   Санкт-Петербургский политехнический университет Петра Великого.
   ОПРЕДЕЛЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В УСЛОВИЯХ НАЛИЧИЯ МЕХАНИЗМОВ САМОЗАЩИТЫ.

9. **Мясников А.В., Москвин Д.А.**
   Санкт-Петербургский политехнический университет Петра Великого.
   ОПТИМИЗАЦИЯ ПРОЦЕССА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ.

10. **Ковылкин Д.С., Трусов Н.А., Фоменко К.Э.**
    Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
    ПОДХОД К МОДЕЛИРОВАНИЮ КОМПЬЮТЕРНЫХ АТАК ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ЭЛЕМЕНТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ.

Обед /13:00 – 14:00/ ресторан «Атриум»

Секция 2, продолжение. Зал «Крестовский 2»
/14:00 – 18:00/

Информационная безопасность: взгляд молодых ученых

Руководители заседания:

Бирюков Д.Н. *Д.т.н., проф., Военно-космическая академия имени А. Ф. Можайского.*

Александрова Е.Б. *Д.т.н., проф., Санкт-Петербургский политехнический университет Петра Великого.*

Полтавцева М.А. *К.т.н., Санкт-Петербургский политехнический университет Петра Великого.*

11. **Трусов Н.А., Головин Д.А., Ковылкин Д.С., Нагибин Д.В.**
Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
АНАЛИЗ ПОДХОДОВ К ПРЕДСТАВЛЕНИЮ, ХРАНЕНИЮ, ОБРАБОТКЕ И ОТОБРАЖЕНИЮ РАЗНОРОДНЫХ ДАННЫХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

12. **Ситников Л.В., Андрушкевич С.С., Бирюков Д.Н.**
Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ПАРАМЕТРОВ ДЛЯ ПРЕДСТАВЛЕНИЯ ЗНАНИЙ ОБ УЯЗВИМОСТЯХ.

13. **Арутюнян Б.А., Туктаров Р.Р., Моргунов В.М.**
Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЭЛЕМЕНТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ, ПУТЁМ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ЛИЦ, ОСНОВАННОЙ НА НЕЙРОННЫХ СЕТЯХ.

14. **Усова М.А.**
Университет ИТМО, Санкт-Петербург.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО ПРОИЗВОДСТВА.

Кофе-брейк /15:45 – 16:15/

15. **Щепин Н.Д.**
Университет ИТМО, Санкт-Петербург.
КОММУНИКАЦИЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ.

16. **Исаева М.А.**
Санкт-Петербургский государственный университет аэрокосмического приборостроения.
МЕТОД ВЫЯВЛЕНИЯ ТИПОВ СТЕГАНОГРАФИЧЕСКИХ АТАК НА ОСНОВЕ «ХРУПКИХ» МЕТОК.

17. **Базгутдинова Э.Р.**
Санкт-Петербургский государственный университет аэрокосмического приборостроения.
АНАЛИЗ СТОЙКОСТИ ПРОТОКОЛОВ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ ПРИ ПОМОЩИ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ ВЕРИФИКАЦИИ.

Ужин /19:00/ ресторан «Атриум»

26 сентября, среда

Завтрак /8:30 – 10:00/ ресторан «Атриум»

Секция 3. Вип-переговорная «Parklane»
/10:00 – 14:00/

Криптографические методы защиты и технология блокчейн

Руководители заседания:

Баранов А.П. *Д.ф-м.н., проф., Заместитель Генерального директора АО ГНИВЦ.*

Матюхин Д.В. *К.ф.-м.н., ФСБ России.*

Александрова Е.Б. *Д.т.н., проф., Санкт-Петербургский политехнический университет Петра Великого.*

---

1. **Архангельский В.Г.**
   ФГАНУ ЦИТИС, г. Москва.
   ОБ ОДНОМ ПОДХОДЕ К ОБЕСПЕЧЕНИЮ ПОДКОНТРОЛЬНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В УСЛОВИЯХ ОТСУТСТВИЯ ДОВЕРЕННЫХ ПОЛЬЗОВАТЕЛЕЙ В МЕСТАХ ЭКСПЛУАТАЦИИ.

2. **Ярмак А.В., Александрова Е.Б.**
   Санкт-Петербургский политехнический университет Петра Великого.
   СХЕМА ИЕРАРХИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ИЗОГЕНИЯХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В СЕТЯХ ДИНАМИЧЕСКОЙ АРХИТЕКТУРЫ.

3. **Сабанов А.Г.**
   МГТУ им. Н.Э. Баумана, ЗАО «Аладдин Р.Д.», г. Москва
   ОБ УРОВНЯХ ДОВЕРИЯ К ПЕРВИЧНОЙ ИДЕНТИФИКАЦИИ.

4. **Шенец Н.Н.**
   Санкт-Петербургский политехнический университет Петра Великого.
   АУТЕНТИФИКАЦИЯ И ВЫРАБОТКА ОБЩЕГО КЛЮЧА НА ОСНОВЕ ГОМОМОРФНОГО РАЗДЕЛЕНИЯ СЕКРЕТА.

5. **Беззатеев С.В.**
   Университет ИТМО, Санкт-Петербургский государственный университет аэрокосмического приборостроения,
   Волошина Н.В.
   Университет ИТМО.
   СИСТЕМЫ РАЗНОТИПНОЙ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ.

Кофе-брейк /11:30 – 11:45/

6. **Комисаренко В.В.**
   ООО «Лайт Вел Организейшн» г. Минск.
   О БЛОКЧЕЙН ПЛАТФОРМАХ НОВОГО ПОКОЛЕНИЯ.
7. **Бабаш А.В, Баранова Е. К.**
   НИУ ВШЭ, г. Москва.
   СОВЕРШЕННЫЕ ШИФРЫ И КАК К НИМ ОТНОСИТЬСЯ. НОВЫЙ СОВЕРШЕННЫЙ ШИФР ТУК-ТУК.

8. **Даниленко А.Ю., Акимова Г.П.**
   ФИЦ ИУ РАН, г. Москва.
   ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН.

9. **Козачок А.В., Копылов С.А.**
   Академия ФСО России, г. Орёл.
   РОБАСТНЫЙ ВОДЯНОЙ ЗНАК КАК СПОСОБ ЗАЩИТЫ ТЕКСТОВЫХ ДАННЫХ.

10. **Шкоркина Е.Н., Александрова Е.Б.**
    Санкт-Петербургский политехнический университет Петра Великого.
    ПРИМЕНЕНИЕ ЛИЧНОСТНЫХ СХЕМ ШИФРОВАНИЯ С ПОДПИСЬЮ СОВМЕСТНО С АУТСОРСИНГОМ В VANET/FANET-СЕТЯХ.

Обед /14:00 – 15:00/ ресторан «Атриум»

Секция 4. Вип-переговорная «Parklane»
/15:00 – 19:00/

Информационная безопасность современных сетевых технологий в условиях цифровизации

Руководители заседания:

Лось В.П. *МОО АЗИ, д.в.н., проф. заведующий кафедрой МИРЭА.*
Зегжда П.Д. *Д.т.н., проф., руководитель отделения «Кибербезопасность» СПбПУ*
Петренко С.А. *Д.т.н., проф., директор по информационной безопасности, Университет Иннополис*
Жуков И.Ю. *Д.т.н., проф., НИЯУ МИФИ, Заместитель генерального директора «Национальный мобильный портал»*

---

1. **Трифаленков И.А.**
   Huawei technologies, Москва.
   СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗВИТИИ ИНТЕРНЕТА ВЕЩЕЙ.

2. **Лускатов И.В., Пилькевич С.В.**
   Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
   МЕТОДИКА ВЫЯВЛЕНИЯ КИБЕРУГРОЗ НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ СЕТИ ИНТЕРНЕТ.

3. **Ададуров С.Е., Ададуров А.С.**
   АО ВНИИЖТ, г. Москва.
   ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ РАБОЧЕЙ ГРУППЫ «КИБЕРБЕЗОПАСНОСТЬ» ЕВРОПЕЙСКОГО СОЮЗА ТРАНСПОРТНОЙ ПОЛИЦИИ И СЛУЖБ БЕЗОПАСНОСТИ ЖЕЛЕЗНЫХ ДОРОГ COLPOFER.

4. **Крундышев В.М., Калинин М.О.**
   Санкт-Петербургский политехнический университет Петра Великого.
   СИСТЕМА АДАПТИВНОГО УПРАВЛЕНИЯ ПРОГРАММНЫМИ СЕРВИСАМИ НА ПЛАТФОРМЕ ЭЛАСТИЧНЫХ ВЫЧИСЛЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ПРОГРАММНО-КОНФИГУРИРУЕМОЙ БЕЗОПАСНОСТИ В СЕТЯХ ТРАНСПОРТНЫХ СРЕДСТВ.

5. **Грушо А.А., Тимонина Е.Е.**
   ФИЦ ИУ РАН, г. Москва.
   ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ ОБЕСПЕЧЕНИЯ СОПРЯЖЕНИЯ КАНАЛОВ ГЕТЕРОГЕННОЙ СЕТИ.

6. **Гнидко К.О.**
   Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
   ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ КВАНТОВОПОДОБНЫХ ФЕНОМЕНОВ НЕПРЯМОГО РАСПРОСТРАНЕНИЯ ЭМОЦИОНАЛЬНО ОКРАШЕННОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ.

Кофе-брейк /16:45 – 17:00/

7. **Пилькевич С.В.**
   Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
   МОДЕЛИРОВАНИЕ КВАНТОВОПОДОБНЫХ СВОЙСТВ ПСИХИКИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ В ПРОЦЕССЕ ПРИНЯТИЯ ИМИ НЕРАЦИОНАЛЬНЫХ РЕШЕНИЙ

8. **Павленко Е.Ю., Зегжда Д.П.**
   Санкт-Петербургский политехнический университет Петра Великого.
   ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ПРИНЦИПОВ ГОМЕОСТАЗА.

9. **Бусыгин А.Г., Коноплев А.С.**
   Санкт-Петербургский политехнический университет Петра Великого.
   АРХИТЕКТУРА УСТОЙЧИВОЙ САМОРЕГУЛИРУЮЩЕЙСЯ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ.

10. **Фоменко К.Э., Бирюков Д.Н.**
    Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
    ПОДХОД К ОЦЕНИВАНИЮ ВАЖНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ.

11. **Единархова А.О.**
    Военно-космическая академия имени А. Ф. Можайского, Санкт-Петербург.
    ПОДХОД К ОПРЕДЕЛЕНИЮ ВЛИЯТЕЛЬНОСТИ ОБЪЕКТОВ И УПРАВЛЕНИЮ РАСПРОСТРАНЕНИЕМ ИНФОРМАЦИИ В НЕБОЛЬШИХ СОЦИАЛЬНЫХ ГРУППАХ.

12. **Кузнецов А.В.**
    НТЦ Вулкан, г. Москва.
    КОМБИНИРОВАННАЯ ОБРАБОТКА ПОТОКОВ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ.

13. **Дахнович А.Д., Москвин Д.А.**
    Санкт-Петербургский политехнический университет Петра Великого.
    ПОДХОД К ОРГАНИЗАЦИИ БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ СЕГМЕНТАМИ СЕТИ ЦИФРОВОГО ПРОИЗВОДСТВА.

14. **Никольский А.В., Зегжда Д.П.**
    Санкт-Петербургский политехнический университет Петра Великого.
    ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИЗОЛЯЦИИ ДЛЯ СОЗДАНИЯ СОВРЕМЕННЫХ ЗАЩИЩЁННЫХ СИСТЕМ.

15. **Калинин М.О.**
    Санкт-Петербургский политехнический университет Петра Великого
    МЕТОДИКА ИССЛЕДОВАНИЯ КИБЕРУГРОЗ В БОЛЬШИХ СИСТЕМАХ ЦИФРОВОЙ ЭКОНОМИКИ.

Ужин /19:00/ ресторан «Атриум»

Секция 5. NeoQUEST.

Соревнование по кибербезопасности

Зал «Крестовский 2»
/11:00 – 19:00/

/10:55/ Приветственное слово ведущего NeoQUEST-2018

/11:00 – 13:00/ Доклады

Илья Петров: «Не доверяй никому, даже своему антивирусу»

Роман Щербаков: «Проблематика встраивания пользовательского кода в проприетарные ОС»

Алексей Никольский: «Генезис: первая секунда жизни компьютера»

Кофе-брейк /13:00 – 13:20/

/13:20 – 15:35/ Доклады

Евгений Федотов, Евгений Бабак: «Ястреб сбит. Исследуем безопасность дронов»

Подсекция коротких докладов Fast Track:

1. Зайцева Наталия: «Ok Google»
2. Дахнович Андрей: «Что Facebook знает о нас? Что мы знаем о Facebook?»
3. Шматов Вадим: «Неочевидное применение проверяемых вычислений»
4. Зайцева Наталия: «Извините, роботов не обслуживаем»

Панков Илья: «Ghostbusters: Spectre & Meltdown»

Подсекция коротких докладов Fast Track (продолжение):

5. Квасенков Иван: «Абсолютная власть: управление процессором через USB»
6. Малышев Егор: «Status: online» часть 1
7. Мясников Алексей: «Status: online» часть 2

/15:35 – 15:55/ Кофе-брейк

/11:00 – 18:00/ Доклады и подведение итогов NeoQUEST-2018:
Cold Boot шоу: атака с использованием жидкого азота

Штыркина Анна, Ярмак Анастасия: «Цифровые подписи и где они обитают»
Шматов Вадим: «Глубокое обучение в стеганографии: we need to go deeper»

Подведение итогов twitter-викторины «ЕГЭ по ИБ»,
квеста «Виноградный Джо, или Как сисадмин Виноград оказался не таким уж неуловимым» от DEF CON, подведение итогов финала hackquest,
награждение победителей

Зал «Крестовский 1»
Воркшопы

/11:00 – 13:00/ Максим Вотчеников: «Эпично Этично пентестим сайты!»

/13:00 – 13:20/ Кофебрейк

/13:20 – 15:35/ Алексей Никольский: «ОС? Не, не слышал»

/15:35 – 15:55/ Кофебрейк

/15:55 – 17:55/ Роман Щербаков: «Шьем с Али. Обзор и применение китайских программаторов»

Киберпространство

/11:00 – 17:55/ онлайн-конкурсы на протяжении всего дня:

1. Twitter-викторина «ЕГЭ по ИБ»:

каждый час в твиттере https://twitter.com/NeoquestSupport выкладываются задания. Для участия нужно сначала прислать на почту support@neoquest.ru свой логин, а затем в течение дня с этой же почты присылать ответы на задания.

Подведение итогов – в конце дня!

2. Квест от команды DEF CON из Нижнего Новгорода «Виноградный Джо, или Как сисадмин Виноград оказался не таким уж неуловимым».

В квесте будет представлен виртуальный мир антиутопии, по которому вам предстоит путешествовать, выполняя различные задания.

Участвовать можно как в одиночку, так и в команде. Сложность большинства заданий — легкая или средняя, к тому же, команда DEF CON весь день будет рядом, готовая дать подсказки.

Подведение итогов NeoQUEST-2018 /18:00/
Закрытие конференции

27 сентября, четверг

Завтрак /8:30 – 10:00/ ресторан «Атриум»

Выезд из отеля /10:00 – 12:00/

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 Российской 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.

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

ГК «СпецПроект»

195197, г. Санкт-Петербург, ул. Жукова, д. 18
Телефон: +7(812) 612-12-36
Факс: +7(812) 612-12-37
М.т.: +7(911) 911-40-55, +7(901) 970-74-57
office@gkspr.ru
www.gkspr.ru

Группа компаний «СпецПроект» успешно работает на рынке информационной безопасности с 2008 года, является одним из ведущих поставщиков комплексных решений по защите информации, в том числе информации, содержащей сведения, составляющие государственную тайну, и имеет все соответствующие лицензии ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации. Предприятия, входящие в нашу Группу компаний, уже поставляют как готовые, так и индивидуальные решения по созданию системы защиты информации в крупнейшие российские предприятия оборонной и гражданской промышленности, а также иным государственным и коммерческим организациям и учреждениям.

Мы оказываем услуги по следующим направлениям:

- защита государственной тайны, включая подготовку к лицензированию учреждений, организаций, предприятий при открытии или перелицензировании своих РСП, а также создание условий для работы с государственной тайной организациям, не имеющим собственных РСП, с последующим сопровождением;
- организация и проведение обучения руководителей и специалистов, ответственных за создание условий по защите государственной тайны, а также в области технической защиты информации и другим направлениям в нашем Учебном центре;
- информационная безопасность, в т.ч. техническая защита информации, сборка и поставка технических средств со специальной проверкой и специальными исследованиями, проектирование систем защиты и проведение работ по обеспечению безопасности любых объектов информатизации (ПДн, ГИС, КИИ, АСУ ТП и др.), системная интеграция, проведение аттестационных испытаний;
- внедрение программного продукта по автоматизации секретного делопроизводства «РСП-Эксперт», предназначенный для компаний, занимающихся в т.ч. работой с секретной документацией.

Профессиональный подход к решению задач любой сложности, накопленный опыт и использование прогрессивных технологий позволяют предлагать нашим клиентам самые современные решения в сфере безопасности и защиты информации.