Программа выступлений на третьей научной школе "Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах" (IM&CTCPA 2017)

Санкт-Петербург, 18 декабря - 21 декабря 2017 г.

СПИИРАН, Санкт-Петербург, 14-я линия В.О., д.39, ауд. 401 (18 декабря)
Университет ИТМО, Санкт-Петербург, ул. Ломоносова, 9, актовый зал (19 - 21 декабря)

http://www.comsec.spb.ru/imctcpa17

18 декабря, Понедельник

Семинар международной лаборатории "Информационная безопасность киберфизических систем" Санкт-Петербургского университета ИТМО.
Председатели:
Котенко Игорь Витальевич, д.т.н., профессор, заведующий лабораторией проблем компьютерной безопасности, СПИИРАН, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия.
Дидье Эльбаз, PhD, руководитель группы распределенных и асинхронных вычислений, Национальный Центр Научных Исследований (CNRS), Тулуза, Франция, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия.

1. Научный семинар **"Проблемы развития интеллектуальных защищенных распределенных автономных робототехнических систем"**.
Модератор:
Дидье Эльбаз, PhD, руководитель группы распределенных и асинхронных вычислений, Национальный Центр Научных Исследований (CNRS), Тулуза, Франция, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия.

2. Научный семинар **"Проблемы безопасности и надежности современных киберфизических систем"**.
Модератор:
Хакима Чаучи, PhD, профессор, институт телекоммуникаций, Париж, Франция.

3. Научный семинар **"Перспективы развития защищенных киберфизических автомобильных систем"**.
Модератор:
Роланд Рике, PhD, заместитель руководителя отдела безопасной инженерии/обеспечения и соответствия требованиям, Фраунхофер, институт безопасных информационных технологий, Дармштард, Германия.

4. Научный семинар **"Формальные подходы к анализу защищенности киберфизических систем"**.
Модератор:
Янник Шевалье, PhD, доцент, университет Пола Сабатье (Тулуза III), Тулуза, Франция.

5. Научный семинар **"Формальные методы для киберфизических систем"**.
Модератор:
Мартин Штрекер, PhD, доцент, университет Пола Сабатье (Тулуза III), Тулуза, Франция.

6. Научный семинар **"Подходы, методы и алгоритмы для контроля доступа киберфизических систем"**.
Модератор:
Владимир Олещук, PhD, профессор, глава группы Коммуникации и Системной Безопасности, отделение информационно-коммуникационных технологий, факультет инженерного дела и науки, университет Агдера, Агдер, Норвегия.

7. Научный семинар **"Методы анализа рисков в киберфизических системах"**.
Модератор:
Фабрицио Байарди, PhD, профессор, университет Пиза, Пиза, Италия.

8. Научный семинар **"Информационная безопасность в кибер-физических системах"**.
Модераторы:
Котенко Игорь Витальевич, д.т.н., профессор, заведующий лабораторией Проблем компьютерной безопасности, СПИИРАН, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия;
Беззатеев Сергей Валентинович, д.т.н., доцент, заведующий кафедрой "Безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия.

19 декабря, Вторник

Время	Название выступления	Лектор
9.00-9.30	Регистрация участников научной школы	
9.30-9.50	- Открытие **Международной научной школы IM&CTCPA 2017** - Вступительное слово	**Котенко Игорь Витальевич**, д.т.н., профессор, заведующий лабораторией Проблем компьютерной безопасности СПИИРАН, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия
Секция 1.1. Председатель – проф., д.т.н. Котенко Игорь Витальевич		
10.00-10.50	Киберфизические системы и различные информационные проблемы в интеллектуальных распределенных автономных роботах	**Дидье Эльбаз**, PhD, руководитель группы распределенных и асинхронных вычислений, Национальный Центр Научных Исследований (CNRS), Тулуза, Франция, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия
11.00-11.50	Безопасность и надежность в эпоху киберфизических систем	**Хакима Чаучи**, PhD, профессор, институт телекоммуникаций, Париж, Франция
12.00-13.00	Обед	
Секция 1.2. Председатель – к.т.н. Чечулин Андрей Алексеевич		
13.00-13.50	Кибербезопасность в Интернете транспортных средств	**Роланд Рике**, PhD, заместитель руководителя отдела безопасной инженерии/обеспечения и соответствия требованиям, Фраунхофер, институт безопасных информационных технологий, Дармштард, Германия
14.00-14.50	Системы конечных выводов для формального анализа приложений безопасности	**Янник Шевалье**, PhD, доцент, университет Пола Сабатье (Тулуза III), Тулуза, Франция
14.50-15.10	Кофе-брейк	
Секция 1.3. Председатель – к.т.н. Десницкий Василий Алексеевич		
15.10-16.00	Моделирование языков программирования с помощью доказательных ассистентов	**Мартин Штрекер**, PhD, доцент, университет Пола Сабатье (Тулуза III), Тулуза, Франция
16.10-17.00	Использование распределенных реестров для оценки и управления риска информационно-коммуникационных технологий	**Фабрицио Байарди**, PhD, профессор, университет г. Пиза, Пиза, Италия

Секция 1.4. Председатель – д.т.н. Беззатеев Сергей Валентинович		
17.10-17.25	Перспективные применения подвижных критически важных систем	**Сергей Андреев,** к.т.н., старший научный сотрудник Технологического университета г. Тампере, Тампере, Финляндия.
17.25-17.40	Прикладная криптография для Смарт карт	**Лукас Малина,** PhD, старший научный сотрудник технического университета г. Брно, Брно, Чехия
17.40-17.55	Вопросы безопасности в технологиях LPWAN	**Радек Фуиджак,** PhD, научный сотрудник технического университета г. Брно, Брно, Чехия
17.55-18.10	Высокоскоростное шифрование с надежной аутентификацией на платформе FPGA	**Давид Смекал,** научный сотрудник технического университета г. Брно, Брно, Чехия

20 декабря, Среда

Время	Название выступления	Лектор
Секция 2.1. Председатель – проф., д.т.н. Саенко Игорь Борисович		
10.00-10.50	Контроль доступа для кибер-физических систем	**Владимир Олещук,** PhD, профессор, руководитель группы Коммуникации и Системной Безопасности, отделение информационно-коммуникационных технологий, факультет инженерного дела и науки, университет г. Агдера, Агдер, Норвегия
11.00-11.50	Технологии больших данных для мониторинга кибербезопасности и управления инцидентами в SIEM-системах	**Котенко Игорь Витальевич**, д.т.н., профессор, заведующий лабораторией проблем компьютерной безопасности СПИИРАН, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия
12.00-13.00	Обед	
Секция 2.2. Председатель – проф., д.т.н. Котенко Игорь Витальевич		
13.00-13.50	Применение системы параллельных потоковых вычислений для обработки больших данных в интересах решения задач корреляции событий безопасности	**Саенко Игорь Борисович**, д.т.н., профессор, ведущий научный сотрудник СПИИРАН, Санкт-Петербург, Россия
14.00-14.50	Управление индустриальными и мобильными киберфизическими системами: актуальные проблемы в контексте безопасности	**Колюбин Сергей Алексеевич**, к.т.н., доцент, и.о. заведующего кафедрой механотроники (МТ), заместитель директора по научно-технологическому форсайту, Мегафакультет КТиУ, Университета ИТМО, Санкт-Петербург, Россия

14.50-15.10	Кофе-брейк	
Секция 2.3. Председатель – к.т.н. Чечулин Андрей Алексеевич		
15.10-16.00	Пример применения интеллектуального анализа данных в обеспечении информационной безопасности: управление соединениями в сетях с помощью метаданных	**Грушо Александр Александрович**, д.ф-мн., профессор, заведующий лабораторией "Информационной безопасности", ИПИ РАН, Москва, Россия
16.10-17.00	Современные концепции управления рисками информационной безопасности	**Минзов Анатолий Степанович**, д.т.н., профессор, профессор кафедры информационной и экономической безопасности НИУ «МЭИ», Москва, Россия
17.10-18.00	Перспективные направления исследований кибератак	**Александр Адамов**, директор NioGuard Security Lab, преподаватель Blekinge Institute of Technology и ХНУРЭ, Харьков, Украина

21 декабря, Четверг

Время	Название выступления	Лектор
Секция 3.1. Председатель – проф., д.т.н. Саенко Игорь Борисович		
10.00-10.50	Протоколы многофакторной аутентификации для киберфизических систем	**Беззатеев Сергей Валентинович**, д.т.н., доцент, заведующий кафедрой "Безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия
11.00-11.50	Обеспечение безопасности телекоммуникационной IT-инфраструктуры ОАО «РЖД»: проблемы и перспективы	**Чернов Андрей Владимирович**, д.т.н., профессор, заведующий кафедрой "Вычислительной техники и АСУ" ФГБОУ ВО РГУПС, Ростов-на-Дону, Россия
12.00-13.00	Обед	
Секция 3.2. Председатель – к.т.н. Десницкий Василий Алексеевич		
13.00-13.50	Безопасность на основе визуализации	**Коломеец Максим Вадимович**, научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН, аспирант Университет ИТМО, Санкт-Петербург, Россия
14.00-14.50	Методика комплексного проектирования защищенных систем на основе встроенных устройств	**Левшун Дмитрий Сергеевич**, научный сотрудник лаборатории СПИИРАН, аспирант, Университет ИТМО, Санкт-Петербург, Россия
14.50-15.10	Кофе-брейк	

15.10-16.00	Метод верификации качества данных в кибер-физических системах на основе социальных механизмов	**Викснин Илья Игоревич**, ассистент кафедры проектирования и безопасности компьютерных систем, Университет ИТМО, Санкт-Петербург, Россия
16.10-16.20	Закрытие научной школы	

Аннотации лекций

1. **Дидье Эльбаз**, PhD, руководитель группы распределенных и асинхронных вычислений, Национальный Центр Научных Исследований (CNRS), Тулуза, Франция, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия. Доклад "**Киберфизические системы и различные проблемы информатики в интеллектуальных распределенных автономных роботах".**

В лекции рассматриваются киберфизические системы и, в частности, интеллектуальные распределенные автономные роботы, такие как интеллектуальные реконфигурируемые конвейеры для завода будущего. Представлены цель, разработки этих модульных роботизированных систем и ряд вопросов, связанных с распределенными алгоритмами управления модулями и их реконфигурацией для адаптации к новым целям, а также к ошибкам в системе. Уделяется внимание некоторым проблемам в области информатики, таким как разработка эффективных распределенных алгоритмов, отказоустойчивость, статистика и безопасность.

2. **Хакима Чаучи**, PhD, профессор, институт телекоммуникаций, Париж, Франция. Доклад **"Безопасность и надежность в эпоху киберфизических систем"**.

Киберфизическая система охватывает набор цифровых процессов, которые могут отслеживать, контролировать и исполняться на физической системе, представленной роботом, автомобилем, дроном или любой системой с критической связью, критическим временем отклика и обработки. В этой лекции поднимаются главные вопросы, связанные с безопасностью киберфизических систем и требованиями безопасности в разных областях, таких как четвертая промышленная революция, безопасность граждан, а также здравоохранение.

3. **Роланд Рике**, PhD, заместитель руководителя отдела безопасной инженерии/обеспечения и соответствия требованиям, Фраунхофер, институт безопасных информационных технологий, Дармштард, Германия. Доклад **" Кибербезопасность в Интернете транспортных средств".**

Интернет транспортных средств - это новая экосистема, состоящая из транспортных средств, подразделений на дорогах и различных других элементов в Интернете услуг и вещей. Однако подключение транспортных средств через различные интерфейсы открывает новые возможности для злоумышленников дистанционно получать доступ к соответствующим подсистемам безопасности внутри подключенный автомобилей. Лекция посвящена выявлению требований безопасности в этом сложном контексте. Этот важный шаг процесса разработки системы безопасности для автомобильных систем и экосистем не только предоставляет входные данные для разработки безопасной архитектуры, но также способствует проверке соответствия безопасности для тестирования и мониторинга времени выполнения.

4. **Янник Шевалье**, PhD, доцент, университет Пола Сабатье (Тулуза III), Тулуза, Франция. Доклад **"Системы конечных выводов для формального анализа приложений безопасности".**

При формальном анализе безопасности приложения или системы необходимо учитывать возможные действия пользователя с плохим поведением или группы лиц, которые в дальнейшем называются злоумышленниками. В частности, при анализе безопасности,

предоставляемой криптографическим протоколом, за пределами безопасности, предоставляемой используемыми криптографическими примитивами, злоумышленник моделируется при помощи набора аксиом в логике первого порядка и использует специальные процедуры проверки, чтобы вычислить, является ли анализируемая система правильной или ошибочной. В большинстве случаев конкретная процедура доказательства заключается в вычислении конечного числа возможных разрешенных форм, лениво удовлетворяющих ограничениям. Будут представлены некоторые примеры и финитные свойства таких систем.

5. **Мартин Штрекер**, PhD, доцент, университет Пола Сабатье (Тулуза III), Тулуза, Франция. Доклад **"Моделирование языков программирования с помощью доказательных ассистентов"**.

Для обеспечения безопасности программных систем становится все более важной точная семантика используемых языков программирования и правильность преобразований языков. Демонстрируется, как семантика языка программирования может быть формально определена при помощи ассистентов (иллюстрируется доказательством Isabelle), как можно обеспечить сохранение семантики во время компиляции и как возможно отображать программы в более абстрактные модели (например, при помощи автоматов), чтобы проводить полностью автоматизированный, но семантически обоснованный анализ.

6. **Фабрицио Байарди**, PhD, профессор, университет г. Пиза, Пиза, Италия. Доклад **"Использование распределенных реестров для оценки и управления риска информационно-коммуникационных технологий"**.

В лекции вводится основное понятие распределенного реестра, его альтернативной версия и различных условий, которые могут быть приняты для сохранения согласованности и целостности этой распределенной структуры данных. Затем обсуждается, как эта структура данных может использоваться при оценке и управлением риском, создаваемым инфраструктурой информационно-коммуникационных технологий (ИКТ). Также рассматривается вопрос о том, как эти мероприятия могут быть реализованы в режиме реального времени.

7. **Сергей Андреев**, к.т.н., старший научный сотрудник Технологического университета г. Тампере, Тампере, Финляндия. Доклад **"Перспективные применения подвижных критически важных систем"**.

По мере формирования коммуникационной технологии пятого поколения (5G) возникает важный вопрос о типах приложений, которые должны быть реализованы быстро развивающейся экосистемой 5G и за ее пределами. Вместе с тем возникают значительные проблемы, связанные с перспективными сферами использования, включающими движущиеся транспортные средства, дроны и промышленные роботы. Комплексная мобильность этих появляющихся критически важных систем требует специализированной коммуникации, позволяющей противостоять существующим решениям безопасности и секретности. Доклад включает краткий обзор недавних достижений результатов исследований и методов поддержки таких приложений следующего поколения для развертывания критически важных систем.

8. **Лукас Малина,** PhD, старший научный сотрудник технического университета г. Брно, Брно, Чехия. Лекция **"Прикладная криптография для Смарт карт".**
Доклад начинается с краткого представления исследовательской группы криптологии университета технологий Брно. В презентации раскрываются вопросы о возможности использования криптографических примитивов могут в рамках смарт-карт. После краткого обзора большинства распространенных платформ, таких как карты JAVA-карты, карты MultOS, базовые карты и карты .NET, в докладе предлагается оценка ECC-примитивов и криптографических операций на картах.

9. **Радек Фуиджак,** PhD, научный сотрудник технического университета г. Брно, Брно, Чехия. Лекция **"Вопросы безопасности в технологиях LPWAN".**
Мы живем в эпоху цифровых технологий, где ежедневно развиваются различные типы коммуникации. В настоящее время мы являемся свидетелями роста средств Интернета вещей. Приходят новые коммуникационные технологии с крайне длинным диапазоном действия, более 10 километров, при этом потребление энергии оказывается достаточно низким, чтобы функционировать без батарей более 10 лет. Помимо того, что эти технологии продвигают идею Интернета вещей, они также приносят большое число проблем на разных уровнях развития и исследований. В докладе раскрываются новые средства и проблемы безопасности в конкретном их применении.

10. **Давид Смекал**, научный сотрудник технического университета г. Брно, Брно, Чехия. Лекция **"Высокоскоростное шифрование с надежной аутентификацией на платформе FPGA"**.
В докладе описывается дизайн системы шифрования с использованием алгоритма AES (Advanced Encryption Standard) с использованием режима GCM (режим счетчика Галуа) и его реализация на платформе FPGA (полевой программируемый логический элемент). Основная цель - описание реализации подсистемы шифрования VHDL для программируемых карт с использованием чипа Xilinx Virtex-7.

11. **Владимир Олещук**, PhD, профессор, глава группы Коммуникации и Системной Безопасности, отделение информационно-коммуникационных технологий, факультет инженерного дела и науки, университет г Агдера, Агдера, Норвегия. Доклад **"Контроль доступа для кибер-физических систем".**
Киберфизические системы (КФС) включают взаимодействие между большим количеством сущностей (как из кибер-мира, так и из физического мира), которые могут охватывать разные области и принадлежности. Они предоставляют услуги и функциональные возможности, которые могут требовать использования знаний об окружающих физических пространствах. Неконтролируемое вскрытие таких знаний или неограниченное взаимодействие между сущностями может быть использовано и и являться причиной серьезных проблем безопасности и секретности. Большинство традиционных подходов редко решают эти проблемы. Необходимы новые модели и механизмы контроля доступа, более адекватные для защиты чувствительных ресурсов от несанкционированного доступа. В лекции рассматриваются проблемы контроля доступа для КФС и примеры решений, которые демонстрируют, как некоторые из этих проблем могут быть преодолены.

12. **Колюбин Сергей Алексеевич**, к.т.н., доцент, И.о. заведующего кафедрой механотроники (МТ), Заместитель директора по научно-технологическому форсайту, Мегафакультет КТиУ, Университета ИТМО, Санкт-Петербург, Россия. Доклад **"Управление индустриальными и мобильными киберфизическими системами: актуальные проблемы в контексте безопасности".**

На лекции будут рассмотрены ключевые технологии, тренды и перспективы развития киберфизических систем, а также сформулированы ключевые требования к их разработке. Актуальные приложения будут рассмотрены, в том числе, в контексте безопасности. Отдельное внимание будет уделено исследованиям в области индустриальных и мобильных киберфизических систем в Университете ИТМО.

13. **Котенко Игорь Витальевич**, д.т.н., профессор, заведующий лабораторией проблем компьютерной безопасности, СПИИРАН, соруководитель международной лаборатории "Информационная безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия. Доклад **"Технологии больших данных для мониторинга кибербезопасности и управления инцидентами в SIEM-системах".**

Рассматривается современное состояние исследований и разработок в области больших данных, представляются модели, методики, методы и средства для использования технологий больших данных в перспективных SIEM-системах. Особенностью рассматриваемых решений является акцент на интеграции технологий больших данных и технологий управления информацией и событиями безопасности. Представлены аспекты обеспечения безопасности технологий больших данных. Приводятся примеры разработанных систем мониторинга безопасности и управления инцидентами, основанных на технологиях больших данных, в том числе коммерческих, open source, исследовательских и собственных разработок. Проводится сравнение различных реализаций систем мониторинга безопасности и управления инцидентами, и намечаются перспективные направления исследований и разработок SIEM-систем, основанных на технологиях больших данных, в том числе предназначенных для мониторинга и управления инцидентами в киберфизических системах.

14. **Грушо Александр Александрович**, д.ф-мн., профессор, заведующий лабораторией "Информационной безопасности", ИПИ РАН, Москва, Россия. Доклад **"Пример применения интеллектуального анализа данных в обеспечении информационной безопасности: управление соединениями в сетях с помощью метаданных".**

Рассматривается задача информационной безопасности при управлении сетевыми соединениями. Акцент делается на использовании метаданных для управления соединениями. Формирование метаданных представляется как задача интеллектуального анализа данных.

15. **Минзов Анатолий Степанович**, д.т.н., профессор, профессор кафедры информационной и экономической безопасности НИУ «МЭИ», Москва, Россия. Доклад **"Современные концепции управления рисками информационной безопасности".**

Сегодня существует несколько концепций создания систем менеджмента информационной безопасности, однако наиболее интересными и распространенными для бизнеса являются концепции на основе управления рисками. Существующий стандарт ГОСТ Р ИСО/МЭК 27005, гармонизированный с Международным стандартом ISO/MEC 27005, даёт лишь общее представление управления рисками в виде рекомендаций. При этом не учитываются связи между отдельными показателями рисков, методы вычисления метрик рисков, механизмы определения способов их обработки. В докладе будут рассмотрены современные алгоритмы

обработки рисков на основе обобщенных многофакторных моделей рисков, включающих экономические оценки затрат на обработку рисков, механизмы выделения агрегатов рисков и их анализа и применение нечетких множеств для вычисления метрик рисков. Результаты применения новых подходов к управлению рисками будут продемонстрированы на имитационной модели управления рисками.

16. **Саенко Игорь Борисович**, д.т.н., профессор, ведущий научный сотрудник, СПИИРАН, Санкт-Петербург, Россия. Доклад **"Применение системы параллельных потоковых вычислений для обработки больших данных в интересах решения задач корреляции событий безопасности"**.
Рассматривается сущность технологии параллельных потоковых вычислений на примере технологии Complex Event Processing, лежащей в основе функционирования программной системы Spark. Обсуждаются математические основы отдельных задач корреляции событий безопасности и алгоритмы реализации их решения в системе Spark. Демонстрируются результаты экспериментальной оценки разработанных метода, алгоритмов и программного прототипа.

17. **Александр Адамов**, директор NioGuard Security Lab, преподаватель Blekinge Institute of Technology и ХНУРЭ, Харьков, Украина. Лекция **"Перспективные направления исследований кибератак"**.
В лекции рассматриваются перспективные направления исследований связанных с анализом кибератак, в том числе и на критическую инфраструктуру. Данные направления включают автоматизацию анализа, извлечение и анализ конфигураций вредоносных программ, созданных на основе SaaS-модели, технологии обхода детектирования с использованием полиморфного шифрования и обфускации кода и противодействия автоматизированным системам анализа, технологии детектирования на основе кластерного анализа дампов трафика и процессов, моделирование кибератак и др.

18. **Беззатеев Сергей Валентинович**, д.т.н., профессор, заведующий кафедрой "Безопасность киберфизических систем", Университет ИТМО, Санкт-Петербург, Россия. Доклад **"Протоколы многофакторной аутентификации для киберфизических систем"**.
Предлагаются протоколы аутентификации, использующие факторы различного типа и назначения. В частности, рассматривается набор факторов, принимающих во внимание местоположение и состояние пользователя, а также факторы, блокирующие процесс аутентификации или необходимые для него. Использование многофакторных систем аутентификации может существенно повысить безопасность и надежность обработки, передачи и хранения данных в кибер-физических системах. Обсуждаются системы многофакторной аутентификации, использующие пороговые схемы. Такой подход даст возможность обеспечить многоуровневый доступ к информации.

19. **Чернов Андрей Владимирович**, д.т.н., профессор, заведующий кафедрой "Вычислительной техники и АСУ" ФГБОУ ВО РГУПС, Ростов-на-Дону, Россия. Доклад **"Обеспечение безопасности телекоммуникационной IT-инфраструктуры ОАО «РЖД»: проблемы и перспективы"**.
В докладе рассматривается современное состояние IT-инфраструктуры ОАО «РЖД». В связи с большим разнообразием IT – технологий, средств телекоммуникаций и связи, автоматизированных рабочих мест, серверных приложений и информационно-

телекоммуникационных услуг, предоставляемых Главным вычислительным центром ОАО «РЖД», в докладе будут рассматриваться вопросы информационной безопасности, касающиеся корпоративной сети передачи данных.

20. **Коломеец Максим Вадимович**, научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН, аспирант, Университет ИТМО, Санкт-Петербург, Россия. Доклад **"Безопасность на основе визуализации".**
Обсуждаются ключевые принципы визуализации данных и их применение в информационной безопасности. Рассматривается история визуальной аналитики, архитектура систем визуализации, модели визуализации с примерами применения в кибер- и киберфизической безопасности, готовые инструменты визуальной аналитики, а также психологические особенности визуального восприятия. Материал лекции направлен на формирование комплексного понимания возможностей визуальной аналитики для анализа данных безопасности, демонстрирует способы абстрагирования физических элементов систем и может послужить необходимым фундаментом для проектирования собственных систем визуального анализа данных безопасности.

21. **Левшун Дмитрий Сергеевич**, научный сотрудник лаборатории СПИИРАН, аспирант, Университет ИТМО, Санкт-Петербург, Россия. Доклад **"Методика комплексного проектирования защищенных систем на основе встроенных устройств".**
Рассматриваются вопросы проектирования защищенных систем на основе встроенных устройств. Анализируются современные подходы к проектированию защищенных встроенных устройств и систем на их основе, а также подходы к разработке безопасного программного обеспечения. Определяются границы их применимости для построения защищенных систем на основе встроенных устройств. Предлагается методика проектирования защищенных систем на основе встроенных устройств, и приводится пример ее применения при разработке комплексной системы киберфизической безопасности.

22. **Викснин Илья Игоревич**, ассистент кафедры проектирования и безопасности компьютерных систем, Университет ИТМО, Санкт-Петербург, Россия. Доклад **"Метод верификации качества данных в кибер-физических системах на основе социальных механизмов".**
Излагается подход к повышению качества частных показателей информационной безопасности в процессе информационного взаимодействия элементов кибер-физической системы. Определяются основные уровни и потоки информационного взаимодействия элементов и специфические механизмы обеспечения защищенного информационного взаимодействия. Предлагается подход к анализу информации, поступающей от элемента-источника, на основе субъективной информации об этом элементе. Вводится мера количественной оценки качества субъективной информации об элементе на основе социальных механизмов, базирующихся на понятиях истинность, репутация и доверие. Демонстрируется эффект снижения времени реакции кибер-физической системы на обнаружение и противодействие скрытого деструктивного информационного воздействия, достигающийся за счет использования предложенного подхода.