«ОБНАРУЖЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА БАЗЕ ПРОГРАММНОГО КОМПЛЕКСА «AMPIRE»

программа повышения квалификации

2025

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОГРАММЫ

Продолжительность обучения	**140 часов**
Документ, выдаваемый после завершения курса	**удостоверение о повышения квалификации**
Форма обучения	**очная, очно-заочная, применение электронного обучения и дистанционных образовательных технологий**
Режим занятий	**без отрыва/с отрывом от работы.**
Категория слушателей (требования к начальным знаниям)	Лица, имеющие высшее образование или среднее специальное образование в области информационных технологий, занятые в должностях специалистов по информационной безопасности предприятий, учреждений, организаций

После прохождения обучения Вы будете:

- уметь использовать программно-аппаратный комплекс ViPNet IDS;
- уметь проводить мониторинг и анализ событий и инцидентов информационной безопасности, в том числе с использованием средств, входящих в состав киберполигона Ampire;
- уметь проводить расследование инцидентов информационной безопасности, оценку защищённости элементов информационных систем и сетей;
- знать подсистемы обнаружения атак, подсистемы защиты от преднамеренных воздействий, контроля целостности информации;
- уметь проводить аудит журналов на предмет попыток НСД и прочих нарушений;
- уметь организовывать поиск и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для
- обеспечения информационной безопасности данных

Учебно-тематический план

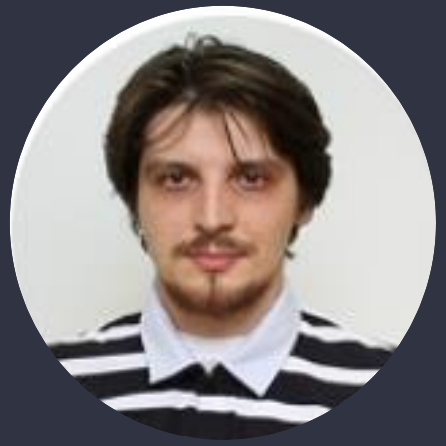
- Модуль 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации.
- Модуль 2. Современные средства анализа и поиска сетевых угроз и уязвимостей программно-аппаратного обеспечения автоматизированных систем.
- Модуль 3. Решения по обнаружению, предотвращению компьютерных атак и интеллектуального анализа событий и автоматического выявления инцидентов на базе продуктов Infotecs.
- Модуль 4. Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire».

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№	Наименование тем и разделов	Всего часов*
1	Модуль 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации.	14
2	Модуль 2. Современные средства анализа и поиска сетевых угроз и уязвимостей программно-аппаратного обеспечения автоматизированных систем.	18
3	Модуль 3. Решения по обнаружению, предотвращению компьютерных атак и интеллектуального анализа событий и автоматического выявления инцидентов на базе продуктов Infotecs.	57
4	Модуль 4. Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire».	40

Примечание: при необходимости количество часов по отдельным модулям программы может быть изменено

АВТОРЫ КУРСА



Подтопельный Владислав Владимирович

старший преподаватель кафедры ИБ

Ильяшов Александр Николаевич

старший преподаватель кафедры ИБ

Как записаться на курс

УЗНАТЬ ПОДРОБНОСТИ И ЗАПИСАТЬСЯ В БЛИЖАЙШУЮ ГРУППУ (ИЛИ НА ИНДИВИДУАЛЬНОЕ ОБУЧЕНИЕ) ВЫ МОЖЕТЕ, ОБРАТИВШИСЬ ПО ЭЛЕКТРОННОЙ ПОЧТЕ:

Кривопускова Екатерина Владимировна,
зам. директора Института цифровых технологий по ДО и ПП

ekaterina.krivopuskova@klgtu.ru

г. Калининград, Советский проспект, 1, каб. 411Г

@KATEKRIVOPUSKOVA