Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

Институт цифровых технологий

УТВЕРЖДАЮ:
Первый проректор

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
00e605f899ce9c3b92f3e8601cfd84a822
Владелец: Огий Оксана Геннадьевна
Действителен: с 16.12.2025 по 11.03.2027

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(программа повышения квалификации)
«Аналитик Security Operations Center (SOC)»

Трудоемкость – 108 ч

Разработчик: *кафедра информационной безопасности*

Авторы: Великите Н.Я., к.ф.-м.н., доцент, доцент
Бабаева А.А., старший преподаватель

г. Калининград
2026

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная профессиональная программа (повышение квалификации), реализуется в соответствии с Федеральным законом от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации", Приказом Минобрнауки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», а также в соответствии с новой системой нормативных правовых актов по охране труда в Российской Федерации, введенных в силу с 01.01.2021 г.

Реализация программы повышения квалификации будет способствовать подготовке специалистов, способных эффективно работать в центре оперативной безопасности (SOC) на позициях аналитиков начального уровня, обладающих знаниями и практическими навыками для мониторинга, обнаружения, анализа и реагирования на киберугрозы.

Цель:	подготовка квалифицированных специалистов, обладающих необходимыми компетенциями для эффективного анализа и реагирования на инциденты информационной безопасности. Программа направлена на формирование практических навыков выявления угроз и управления процессами защиты информационных ресурсов организации и на отработку навыков организации реагирования на инциденты ИБ
Задачи:	Формирование компетенций, необходимых для эффективной работы аналитиком Security Operations Center (SOC). Изучение современных подходов и методов анализа киберинцидентов. Развитие практических навыков выявления угроз информационной безопасности и проработка алгоритмов группового взаимодействия. Овладение инструментами мониторинга и реагирования на инциденты. Настройка и корректировки средств защиты информации для повышения уровня защищенности ИС организации. Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire» (киберполигон).
Категория слушателей. (требования к квалификации слушателей):	Среднее профессиональное образование - программы подготовки специалистов среднего звена по профилю деятельности Высшее образование – бакалавриат или специалитет в области информационной безопасности. Для должностей с категорией - опыт работы в должности с более низкой (техника по защите информации) категорией не менее одного года
Срок освоения:	108 ч.
Режим занятий:	Без отрыва/с отрывом от работы.
Форма обучения	очная, очно-заочная, заочная, применение электронного обучения и дистанционных образовательных технологий.

Планируемые результаты обучения. Компетентностный профиль программы.

Перечень компетенций, подлежащих совершенствованию, и (или) перечень новых компетенций, формирующихся в результате освоения.

ПК-1 Способность организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-1.1 Выявляет признаки атак и аномалий в сетевом трафике и событиях систем мониторинга; проводит комплексный анализа инцидентов информационной безопасности и выявление потенциальных угроз.

ПК-1.2 Организует процесс быстрого реагирования на инциденты информационной безопасности; разрабатывает и внедряет меры по минимизации последствий нарушений информационной безопасности.

Программа обучения разработана на основании профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н

ОТФ: Обслуживание систем защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

ТФ (A/02.5) Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем

Знания: Основные методические и руководящие документы федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;
Нормативные правовые акты в области защиты информации

Умения: Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации

Трудовые действия: Ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем
Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем
Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем

ОТФ: Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации.

ТФ (B/01.6) Диагностика систем защиты информации автоматизированных систем

Знания: Нормативные правовые акты в области защиты информации
Регламент учета выявленных инцидентов
Регламент устранения последствий инцидентов

Умения: Определять источники и причины возникновения инцидентов
Оценивать последствия выявленных инцидентов
Обнаруживать нарушения правил разграничения доступа

Трудовые действия: Обнаружение инцидентов в процессе эксплуатации автоматизированной системы

Идентификация инцидентов в процессе эксплуатации автоматизированной системы

Устранение последствий инцидентов, возникших в процессе эксплуатации автоматизированной системы

2. УЧЕБНЫЙ ПЛАН И КАЛЕНДАРНЫЙ УЧЕБНЫЙ ПЛАН

2.1 Учебный план

№	Наименование предметов, курсов, дисциплин (модулей)	Всего часов	в том числе			Форма контроля
			ЛК	ПЗ	СР	
1	**Модуль 1.** Введение в SOC. Фундамент операционной безопасности. Методологии Mitre ATT&CK, Cyber Kill Chain.	24	12	4	8	Тестирование
2	**Модуль 2.** Инструментарий аналитика SOC. Анализ журналов событий. Дашборды в SOC.	36	16	8	12	Контроль на ПЗ
3	**Модуль 3.** Процессы реагирования. Мапинг по матрицам MITRE. Киберполигон «AMPIRE», разбор сценариев.	40	10	20	10	Контроль на ПЗ
4	**Итоговая аттестация**	8	-	4	4	Выполнение практического кейса
ИТОГО		**108**	**38**	**36**	**34**	

2.2 Календарный учебный график

№ п/п	Наименование предметов, курсов, дисциплин (модулей)	Номер дня 1-й учебной недели с начала обучения[1]					Номер дня 2-й учебной недели с начала обучения					Номер дня 3-й учебной недели с начала обучения				
		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
		4 часа в день					6 часов в день					6 часов в день				
1	**Модуль 1.** Введение в SOC. Фундамент операционной безопасности. Методологии Mitre ATT&CK, Cyber Kill Chain.	Т	Т	Т	П	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х
2	**Модуль 2**. Инструментарий аналитика SOC. Анализ журналов событий. Дашборды в SOC.	Х	Х	Х	Х	Т	Т	Т	Т/ П	Т/ П	Х	Х	Х	Х	Х	Х
3	**Модуль 3.** Процессы реагирования. Мапинг по матрицам MITRE. Киберполигон «AMPIRE», разбор сценариев.	Х	Х	Х	Х	Х	Х	Х	Х	Х	Т	Т/ П	П	П	П	П
4	**Итоговая аттестация**															И

[1]Даты обучения будут определены в расписании занятий при наборе группы на обучение

□ – учебная неделя; Т – теоретическое обучение; И –итоговая аттестация; × – нет недели

3. РАБОЧИЕ ПРОГРАММЫ ПРЕДМЕТОВ, КУРСОВ, ДИСЦИПЛИН (МОДУЛЕЙ) ПРОГРАММЫ

3.1 Рабочая программа модуля «Введение в SOC. Фундамент операционной безопасности. Методологии Mitre ATT&CK, Cyber Kill Chain»

3.1.1 Пояснительная записка

Цель:	формирование у слушателей целостного понимания основ SOC и кибербезопасности; освоение ключевые понятия и структуры SOC, что позволит оценить роль аналитика SOC в обеспечении безопасности информации
В результате изучения слушатели должны:	
знать:	Основы организации и функционирования SOC. Основные киберугрозы и атаки, модели угроз (Kill Chain, MITRE ATT&CK). Фундамент операционной безопасности: определение требований, регулярный мониторинг, контроль доступа, обучение персонала, обеспечение надежности хранения данных и поддержание актуальной конфигурации системы; ключевые технологии и инструменты, используемые в SOC (SIEM, IDS/IPS, EDR, антивирусы, системы анализа трафика). Процессы и процедуры SOC: мониторинг, классификация событий, эскалация инцидентов, основы расследования инцидентов.
уметь:	Выявлять и классифицировать инциденты информационной безопасности. Выполнять первоначальное реагирование на инциденты и следовать процедурам эскалации.
владеть:	Технологией мониторинга, анализа событий и инцидентов информационной безопасности. Навыками анализа сетевого трафика с помощью Wireshark, tcpdump и др. Навыками анализа вредоносного ПО на базовом уровне (статический и динамический анализ). Навыками использования EDR-решений для расследования инцидентов.

3.1.2 Учебно-тематический план

№	Наименование тем и разделов	Всего часов	В том числе			Проверка знаний
			ЛК	ПЗ	СР	
1	Роль и место SOC в структуре безопасности организации.	6	4	-	2	Тестирование
2	Фреймворк MITRE ATT&CK: Жизненный цикл кибератаки (Kill Chain).	6	4	-	2	
3	Фундамент операционной безопасности. Используемые технологии.	6	4	-	2	
4	Первое знакомство с угрозой.	6	-	4	2	
Итого		**24**	**12**	**4**	**8**	

3.1.3 Содержание программы

Наименование темы	Содержание темы
Роль и место SOC в структуре безопасности организации.	Основы организации и функционирования SOC. Модели зрелости SOC. Процессы: мониторинг, анализ, эскалация. Карьерная лестница в SOC. Необходимые "мягкие" навыки (soft skills).
Фреймворк MITRE ATT&CK: Жизненный цикл кибератаки (Kill Chain).	Структура, тактики, техники, матрицы, использование для расследования и проактивного поиска. Анализ цепочки атаки от разведки до достижения цели.
Фундамент операционной безопасности. Ключевые технологии	Типичные сценарии использования расширенной подсистемы аудита событий. Ключевые технологии: Системы управления информацией и событиями безопасности (Security Information and Event Management). IDS / IPS (Intrusion Detection System / Intrusion Prevention System)-средства обнаружения вторжений и предотвращения вторжения, предназначенные для выявления аномалий и угроз, исходящих извне и изнутри инфраструктуры. EDR (Endpoint Detection and Response) - решения для защиты конечных точек (рабочих станций, серверов), обеспечивающие обнаружение и реагирование на угрозы в режиме реального времени.
Первое знакомство с угрозой.	Глубокая разборка сетевых протоколов (TCP/IP, DNS, HTTP/S) для аналитика. Анализ сетевого трафика в Wireshark. Анализ дампа трафика и логов с признаками компрометаци

3.1.4 Промежуточная аттестация по программе

Промежуточная аттестация по модулю проводится в форме тестирования

3.1.5 Обеспеченность образовательного процесса учебной литературой и информационными ресурсами

Материалы для самостоятельной работы и подготовки итогового проекта размещаются на http://eios.klgtu.ru/mod ЭИОС КГТУ. Доступ к материалам осуществляется после регистрации на основании договора об оказании образовательных услуг по программе ДПО.

3.2 Рабочая программа модуля «Инструментарий аналитика SOC. Анализ журналов событий. Дашборды в SOC»

3.2.1 Пояснительная записка

Цель:	сформировать у слушателя навыки использования инструментов аналитика SOC.
В результате изучения слушатели должны:	
знать:	Снифферы (визуальный и экспертный анализ). Системы обнаружения вторжений (хостового типа и сетевые). Системы типа SIEM - ПО для анализа информации, собранной из различных источников для раннего обнаружения инцидентов (Max Patrol, Wazuh). Межсетевые экраны. Основы операционных систем (Windows, Linux) для аналитика: ключевые логи, процессы, реестр, файловая система. Применение Дашбордов в области ИБ

уметь:	Проводить разборку сетевых протоколов (TCP/IP, DNS, HTTP/S), анализ сетевого трафика в Wireshark, анализ трафика и хостовых артефактов.
владеть:	Базовыми навыками анализа вредоносного ПО. Анализом дампа трафика и логов с признаками компрометации

3.2.2 Учебно-тематический план

№	Наименование тем и разделов	Всего часов	В том числе			Проверка знаний
			ЛК	ПЗ	СР	
1	Средства анализа сетевых пакетов.	9	6	-	3	Тестирование
2	Системы обнаружения и предотвращения вторжений (IDS/IPS), фаерволлы. Анализ срабатываний.	9	6	-	3	
3	Анализ журналов событий	7	4	-	3	
4	Расследование инцидента. Дешифровка и анализ вредоносных файлов	11	-	8	3	
	Итого	**36**	**16**	**8**	**12**	

3.2.3 Содержание программы

Наименование темы	Содержание темы
Средства анализа сетевых пакетов.	Способы применения сетевых сенсоров для анализа трафика: NMAP. Средства анализа сетевых пакетов WARESHARK.
Системы обнаружения и предотвращения вторжений (IDS/IPS), фаерволлы. Анализ срабатываний.	Виды систем обнаружений вторжений. Классификация по способам реагирования. Классификация по способам размещения. Классификация по методам анализа. Основные функции и принцип работы IDS NS. Состав, характеристики. Методы анализа срабатываний с использованием Дашбордов
Анализ журналов событий	Просмотр основных журналов событий ОС Windows, Linux, Web-серверов. Мониторинг событий. Настройка журнала.
Расследование инцидента. Дешифровка и анализ вредоносных файлов	Этапы сбора доказательств, сдерживания, ликвидации последствий и анализа. Статический анализ (изучение кода без запуска) и динамический (запуск в изолированной среде для понимания поведения вредоносного файла.

3.2.4 Промежуточная аттестация по программе

Промежуточная аттестация по модулю проводится в форме тестирования

3.2.5 Обеспеченность образовательного процесса учебной литературой и информационными ресурсами

Материалы для самостоятельной работы и подготовки итогового проекта размещаются на http://eios.klgtu.ru/mod ЭИОС КГТУ. Доступ к материалам осуществляется после регистрации на основании договора об оказании образовательных услуг по программе ДПО.

3.3 Рабочая программа модуля «Процессы реагирования. Мапинг по матрицам MITRE. Киберполигон «AMPIRE», разбор сценариев».

3.3.1 Пояснительная записка

Цель:	разобрать процесс реагирования на примере инфраструктуры предприятия, включая мониторинг, анализ инцидента, реагирование с устранением последствий атаки
В результате изучения слушатели должны:	
знать:	Этапы реагирования на инцидент по матрице MITRE. Знать инфраструктуру киберполигона «AMPIRE», принцип работы, форматы, шаблоны.
уметь:	Работать с инцидентами в реальном времени. Работать в команде по выявлению и устранению атак на инфраструктуру.
владеть:	Практическими навыками в реагировании на инциденты.

3.3.2 Учебно-тематический план

№	Наименование тем и разделов	Всего часов	В том числе			Проверка знаний
			ЛК	ПЗ	СР	
1	Процессы реагирования. Мапинг по матрицам MITRE	7	5	-	2	Тестирование
2	Киберполигон «AMPIRE»	7	5	-	2	
3	Разбор сценария №1	13	-	10	3	
4	Разбор сценария №2	13	-	10	3	
Итого		**40**	**10**	**20**	**10**	

3.3.3 Содержание программы

Наименование темы	Содержание темы
Процессы реагирования. Мапинг по матрицам MITRE	Формат Blue Team в ПК Ampire, формат CSIRT в ПК Ampire. Воркшоп по симуляции инцидента и анализу
Киберполигон «AMPIRE»	Основное назначение ПК «Ampire», состав. Функциональные возможности. Типовой шаблон. Группа реагирования. Группа мониторинга (защиты). Цели, задачи. Критерии оценки. Мониторинг и анализ событий информационной безопасности. Шаблон, структура информационной системы предприятия. Карточки инцидентов информационной безопасности, создание и особенности заполнения. Описание интерфейса ПК «Ampire». Распределение по группам. Панель тренировки. Статус уязвимостей. Сценарий тренировки - легенда киберучений.
Разбор сценария №1	Удаленное подключение к сетевому сенсору ПАК ViPNet IDS, Т Мониторинг, анализ и расследование инцидентов информационной безопасности. Просмотр и поиск записей журнала событий. Поиск инцидентов ИБ. Пошаговое отслеживание действий виртуального нарушителя в инфраструктуре предприятия. Экспорт файлов об инциденте. Создание карточки инцидента ИБ.

Разбор сценария №2	Удаленное подключение к информационной структуре предприятия в соответствии с шаблоном. Работа в составе команды. Анализ и распределение карточек инцидентов ИБ. Пошаговый анализ действий виртуального нарушителя в инфраструктуре предприятия и их последствий, Выявление угроз безопасности информации и технических каналов утечки информации, обследование объекта ИС. Работа со специальным программным обеспечением для обнаружения и анализа событий ИБ. Устранение обнаруженных уязвимостей в ИС предприятия. Реализации защитных мер по устранению найденных недостатков ИБ.

3.3.4 Промежуточная аттестация по программе

Промежуточная аттестация по модулю проводится в форме выполнения практического кейса.

3.3.5 Обеспеченность образовательного процесса учебной литературой и информационными ресурсами

Материалы настоящей ДПП предполагается разместить на http://eios.klgtu.ru/mod ЭИОС КГТУ. Доступ к материалам осуществляется после регистрации на основании договора об оказании образовательных услуг по программе ДПП.

В ходе обучения могут использоваться следующие материалы.

1. Методические материалы для работы с программным комплексом обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire»
2. Кузьмин О.В., Чефранова А.О., Фефилов А.В. Безопасность КИИ. – М., 2020. – 326 с.
3. Руководство администратора. Программно-аппаратный комплекс ViPNet TIAS
4. Выписка из руководства администратора. Программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS NS
5. Методический документ/ Методика оценки угроз безопасности информации (утвержден ФСТЭК России 5.02.2021).
6. Документация на продукты ViPNet представлена в виде pdf-файлов на сайте https://infotecs.ru/downloads/documentacii/
7. Банк данных угроз безопасности информации (https://bdu.fstec.ru/)
8. Дополнительные материалы и учебно-методические комплексы на сайте:
   https://infotecs-edu.ru/materials/
   https://infotecs-edu.ru/kompleksy/
9. Платформа VulDB - база данных уязвимостей https://vuldb.com/
10. Веб-интерфейс для данных об уязвимостях CVE https://www.cvedetails.com/
11. Поиск информации/ База знаний на www.opennet.ru
https://www.opennet.ru/search.shtml
12. База знаний о тактике и методах нарушителей https://attack.mitre.org/
13. Материалы базовых сценариев (zip-архивы);
14. Презентации по сценариям киберучений.

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

4.1. Материально-техническое обеспечение учебного процесса

В ходе освоения программы слушатели используют возможности интерактивной коммуникации со всеми участниками и заинтересованными сторонами образовательного процесса, ресурсы и информационные технологии посредством электронной информационной образовательной среды университета.

Перечень современных профессиональных баз данных и информационных справочных систем, к которым обучающимся по образовательной программе обеспечивается доступ (удаленный доступ) является ежегодно обновляемым приложением к рабочим программам дисциплин (рассматривается УМС и утверждается отдельно) и размещается на официальном сайте в разделе «Образовательные программы высшего образования университета» и в ЭИОС.

При дистанционном обучении преподавателю обеспечивается доступ к платформе проведения вебинаров в соответствии с расписанием. Технические и программные средства обеспечиваются слушателем самостоятельно.

Занятия проводятся в компьютерном классе ауд.363 ГУК:

– персональный компьютер с ОС Астра Линукс;

– проектор;

– программное обеспечение «AMPIRE»;

– доступ в сеть Интернет.

При всех формах реализации программы должны соблюдаться требования соответствующих СанПиН.

4.2. Организация образовательного процесса

Реализация программы осуществляется в соответствии с требованиями к организации образовательного процесса в университете, изложенными в локальных нормативных актах.

Приведенное выше распределение модулей и тем занятий по дням занятий может уточняться с учетом выбранной формы обучения (очной, очно-заочной, заочной с применением электронного обучения и дистанционных образовательных технологий).

Обучение осуществляется на образовательной площадке университета и носит непрерывный характер. Преподаватели консультируют слушателей как в очном режиме, так и в режиме онлайн.

Программа разработана на основе практико-ориентированного подхода. Её освоение позволит слушателям решать на современном уровне практические задачи, связанные с функциями по обеспечению требований по защите информации в своих организациях.

4.3. Кадровое обеспечение

Реализация программы обеспечивается профессорско-преподавательским составом, отвечающим одному из следующих критериев:

– наличие ученой степени (ученого звания) по направлению читаемых дисциплин;

– наличие опыта практической работы не менее 3 лет по направлению дисциплины и опыта преподавательской работы не менее 2 лет.

К реализации программы привлекаются как штатные преподаватели университета, так и сторонние специалисты по договорам гражданско-правового характера.

4.4. Методические рекомендации по реализации программы

Лекционные и практические занятия проводятся на базе аудиторного фонда университета.

Для успешного овладения курсом слушателям рекомендуется:

1. Принимать участие во всех лекционных, лабораторных и практических занятиях;
2. Все рассматриваемые на лекциях, лабораторных и практических занятиях вопросы фиксировать либо на бумажных, либо электронных носителях (вести конспект);
3. Обязательно выполнять все рекомендации по самостоятельной работе, получаемые на учебных занятиях;
4. В случае пропуска занятий восполнить пропущенные темы самостоятельно по материалам дисциплины.

Преподавателю следует акцентировать внимание на перечисленных условиях, при проведении занятий в форме ВКС обязательно провести инструктаж слушателей по техническим аспектам подключения к платформе, разъяснить порядок работы с ЭИОС.

5. ИТОГОВАЯ АТТЕСТАЦИЯ ПО ПРОГРАММЕ

Итоговая аттестация реализована в формате проведения киберучения по одному из сценариев, реализованных в ПАК «AMPIRE».

Лицам, успешно освоившим ДПП и прошедшим итоговую аттестацию, выдается документ о повышении квалификации, оформляемый на специальном бланке за подписью ректора университета.

ЛИСТ СОГЛАСОВАНИЯ

Программа дополнительной профессиональной программы (программа повышения квалификации) **«Аналитик Security Operations Center (SOC)»** утверждена на заседании учебно-методической комиссии Института цифровых технологий.

Зам. директора Института
цифровых технологий по ДО и ПП  Е.В. Кривопускова