# ПРОГРАММА КУРСА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
# «РЕЗУЛЬТАТИВНАЯ КИБЕРБЕЗОПАСНОСТЬ»

| № п/п | Наименование учебных модулей, тем | Всего часов |
|---|---|---|
| 1.1 | Учебный модуль №1. Нормативная база, регулирующая информационную безопасность (ФЗ 152, ФЗ 187) и аудит информационной безопасности | 10 |
| 1.2 | Тема №1. Обзор законодательства в области кибербезопасности в России | - |
| 1.3 | Тема №2. Аудит информационной безопасности | - |
| 2. | Тема №3. Роль Docshell в автоматизации учета документов по информационной безопасности | - |
| 2.1 | Учебный модуль №2. Основные классы IT-продуктов для обеспечения эффективной кибербезопасности | 9 |
| 2.2 | Тема №1. Тренды рынка кибербезопаности | - |
| 2.3 | Тема №2. Обзор основных классов IT-продуктов для обеспечения эффективной кибербезопасности | - |
| 3. | Тема №3. Как построить эффективную систему обеспечения ИБ объектов КИИ | - |
| 3.1 | Учебный модуль №3. Результативная кибербезопасность: анализ рисков и выявление недопустимых событий | 14 |
| 3.2 | Тема №1. Методы анализа рисков в области кибербезопасности | - |
| 4. | Тема №2. Выявление недопустимых событий и разработка мер по их предотвращению | - |
| 4.1 | Учебный модуль №4. «Приземление» недопустимых событий, кибертрансформация и разработка плана кибертрансформации | 10 |
| 4.2 | Тема №1. «Приземление» недопустимых событий на IT-инфраструктуру | - |
| 5. | Тема №2. Выстраивание процессов и работы подразделений ИТ и ИБ | - |
| 5.1 | Учебный модуль №5. Харденинг IT-инфраструктуры. Обучение практикам кибербезопасности | 7 |
| 5.2 | Тема №1. Харденинг IT-инфраструктуры | - |
| 6. | Тема №2. Обучение практикам кибербезопасности | - |
| 6.1 | Учебный модуль №6. Проверка защищенности | 11 |
| 6.2 | Тема №1. Выбор способа оценки защищенности | - |
| 6.3 | Тема №2. Этапы оценки защищенности | - |
| 7. | Тема №3. Верификация недопустимых событий и проведение киберучений | - |
| 7.1 | Учебный модуль №7. Мониторинг и реагирование на инциденты | 9 |
| 7.2 | Тема №1. Создание центра противодействия киберугрозам | - |
| 7.3 | Тема №2. Мониторинг событий и реагирование на инциденты ИБ | - |
| 8. | Тема №3. Что делать после инцидента | - |
| 8.1 | Учебный модуль №8. Оценка эффективности, Поддержание киберустойчивости и Запуск программы bug bounty | 10 |
| 8.2 | Тема №1. Оценка эффективности: Метрики результативной кибербезопасности | - |
| 8.3 | Тема №2. Поддержание киберустойчивости: необходимые процессы | - |
| 9. | Тема №3. Запуск программы bug bounty | - |
| Итого: | Итоговая аттестация: подготовка и защита выпускного квалификационного задания | 10 |
| | | **90** |

## Содержание модулей и тем курса

| № | Наименование модуля | Наименование темы | Содержание раздела (темы) | Форма текущего контроля |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 1 | Учебный модуль №1. Нормативная база, регулирующая информационную безопасность (ФЗ 152, ФЗ 187) и аудит информационной безопасности | Тема №1. Обзор законодательства в области кибербезопасности в России | Обязательные требования и рекомендации<br>Регуляторы кибербезопасности<br>Требования по защите информации к ИС, средствам и процессам защиты информации | Тестирование |
| | | Тема №2. Аудит информационной безопасности | Уровни компетенций сотрудников<br>Особенности проведения аудита | Практические занятия |
| | | Тема №3. Роль Docshell в автоматизации учета документов по информационной безопасности | Роль Docshell в автоматизации учета документов по информационной безопасности | Практические занятия |
| 2 | Учебный модуль №2. Основные классы IT-продуктов для обеспечения эффективной кибербезопасности | Тема №1. Тренды рынка кибербезопаности | Технологии: идентификация, обнаружение и предотвращение<br>Архитектура ЦПК<br>Реализации ИБ собственные средства, аутсорсинг специалистов и аренда инструментов | Тестирование |
| | | Тема №2. Обзор основных классов IT-продуктов для обеспечения эффективной кибербезопасности | 5 уровней решений<br>Подробнее про каждый тип решения | Тестирование |
| | | Тема №3. Как построить эффективную систему обеспечения ИБ объектов КИИ | Нормативная база формирования СОИБ<br>Силы СОИБ<br>Состав организационно-распорядительной документации<br>СОИБ Процессы управления СОИБ<br>Средства защиты СБОКИИ<br>Архитектурная карта средств защиты СБОКИИ<br>Этапы построения работающей СОИБ | Семинар |
| 3 | Учебный модуль №3. Результативная кибербезопасность: анализ рисков и выявление недопустимых событий | Тема №1. Методы анализа рисков в области кибербезопасности | Основные понятия ИБ<br>СМИБ<br>Анализ и управление рисками<br>Порядок использования политик, стандартов и руководств | Тестирование. Практические занятия |

| № | Наименование модуля | Наименование темы | Содержание раздела (темы) | Форма текущего контроля |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | Оценка рисков | |
| | | Тема №2. Выявление недопустимых событий и разработка мер по их предотвращению | Обзор методологии<br>Основные домены | Тестирование. Практические занятия |
| | Учебный модуль №4. «Приземление» недопустимых событий, кибертрансформация и разработка плана кибертрансформации | Тема №1. «Приземление» недопустимых событий на IT-инфраструктуру | Как правильно провести инвентаризацию IT-активов для выявления ключевых систем и точек проникновения<br>Какие критерии используются для определения ключевых систем и точек проникновения в IT-инфраструктуре<br>Как соотнести целевые системы с бизнес-процессами для минимизации рисков и увеличения безопасности | Тестирование. Практические занятия |
| | | Тема №2. Выстраивание процессов и работы подразделений ИТ и ИБ | Определение критически значимых бизнес-процессов<br>Реинжиниринг бизнес-процессов<br>Обзор процессов для построения кибербезопасности в организации<br>Основные процессы кибербезопасности<br>Рекомендации по контролю изменений в IT-инфраструктуре<br>Как процесс управления IT-активами связан с кибербезопасностью | Тестирование. Практические занятия |
| 5 | Учебный модуль №5. Харденинг IT-инфраструктуры. Обучение практикам кибербезопасности | Тема №1. Харденинг IT-инфраструктуры | Выстраивание процесса харденинга в организации<br>Харденинг на уровне сетей связи<br>Харденинг на уровне операционной системы и прикладных программ<br>Харденинг на уровне веб-ресурсов<br>Харденинг на уровне доменной инфраструктуры<br>Харденинг на уровне сред виртуализации и облачных сервисов | Тестирование |

| № | Наименование модуля | Наименование темы | Содержание раздела (темы) | Форма текущего контроля |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | Тема №2. Обучение практикам кибербезопасности | Аспекты кибербезопасности, которые необходимо знать всем сотрудникам | Тестирование |
| 6 | Учебный модуль №6. Проверка защищенности | Тема №1. Выбор способа оценки защищенности | Виды работ по оценке защищенности и как выбрать правильный<br>Способы проверки недопустимых событий на практике<br>Сравнение работ по тестированию на проникновение<br>Сравнение работ по анализу защищенности<br>Отличия верификации недопустимых событий от классического тестирования на проникновение | Тестирование |
| | | Тема №2. Этапы оценки защищенности | Определение необходимости и периодичности проведения работ по оценке защищенности<br>Разработка технического задания на работы по оценке защищенности Выбор исполнителя работ по оценке защищенности<br>Выбор ответственного за взаимодействие с исполнителем работ по оценке защищенности<br>Факторы, влияющие на эффективность работ по оценке защищенности<br>Способы безопасного тестирования критически значимых информационных систем<br>Содержание отчета по результатам оценки защищенности<br>Критерии качества работ по оценке защищенности<br>Способы использования результатов работ по оценке защищенности | Тестирование |
| | | Тема №3. Верификация недопустимых событий и проведение киберучений | Порядок проведения верификации недопустимых событий<br>Порядок проведения киберучений | Лабораторная работа |
| 7 | Учебный модуль №7. Мониторинг и реагирование на инциденты | Тема №1. Создание центра противодействия киберугрозам | Центр противодействия киберугрозам и его отличия от SOC<br>Принципы построения центра противодействия киберугрозам | Тестирование |

| № | Наименование модуля | Наименование темы | Содержание раздела (темы) | Форма текущего контроля |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | Тема №2. Мониторинг событий и реагирование на инциденты ИБ | Мониторинг событий кибербезопасности<br>Построение процесса реагирования на инциденты информационной безопасности: базовые принципы<br>Какие документы необходимы для запуска процесса реагирования на инциденты ИБ<br>Как сформировать команду мониторинга и реагирования<br>Какие связи необходимы команде мониторинга и реагирования для эффективной работы<br>Подготовка к реагированию на инциденты ИБ<br>Рекомендации по работе с карточкой инцидента ИБ | Тестирование |
| | | Тема №3. Что делать после инцидента | Финансовая сторона инцидента ИБ<br>Как общаться с внешним миром, если вас взломали | Лабораторная работа |
| 8 | Учебный модуль №8. Оценка эффективности, Поддержание киберустойчивости и Запуск программы bug bounty | Тема №1. Оценка эффективности: Метрики результативной кибербезопасности | Методика экспресс-оценки уровня кибербезопасности организации<br>Как оценить готовность организации к отражению кибертатак<br>Метрики оценки результатов верификации недопустимых событий и киберучений | Тестирование |
| | | Тема №2. Поддержание киберустойчивости: необходимые процессы | Поддержание перечня недопустимых событий в актуальном состоянии | Тестирование |
| | | Тема №3. Запуск программы bug bounty | Определение формата программы bug bounty<br>Подготовка к запуску программы bug bounty<br>Определение размера вознаграждения<br>Верификация отчетов по программе bug bounty | Лабораторная работа |