

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

**АУДИТ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ**

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»


Квалификация (степень) выпускника: Бакалавр

**Кострома**

Рабочая программа дисциплины «Аудит защищенности объектов информатизации» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

Год начала подготовки 2017

Разработал  Алексеев Дмитрий Станиславович, доцент кафедры защиты информации, к.т.н.

Рецензент:  Щекочихин Олег Владимирович, к.т.н., доцент, заведующий кафедрой защиты информации

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

  
Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

  
Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 11 от 30.05.2019 г.

Заведующий кафедрой защиты информации

  
Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 8 от 6.04.2020 г.

Заведующий кафедрой защиты информации

Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 6 от 22.01.2021 г.

Заведующий кафедрой защиты информации

Щекочихин Олег Владимирович, к.т.н., доцент

## 1. Цели и задачи освоения дисциплины

**Целями дисциплины** «Аудит защищенности объектов информатизации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе организации и проведения аудита защищенности объектов информатизации.

Предмет курса - объекты информатизации, технологии аудита защищенности объектов информатизации.

Профессиональные цели курса - формирование знаний в области технологий аудита защищенности объектов информатизации.

Задачи дисциплины:

- изучение основных понятий аудита защищенности объектов информатизации;
- изучение процессного подхода к организации информационной безопасности;
- изучение основных требований к содержанию аудита защищенности объектов информатизации;
- изучение основ контроля и проверки процессов и систем;
- изучение методов оценивания информационной безопасности.

## 2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

### **знать**

- основные понятия аудита защищенности объектов информатизации;
- процессный подход к организации информационной безопасности;
- содержание циклической модели менеджмента качества процессов и систем;
- правовые и методологические основы аудита защищенности объектов информатизации;
- правовые аспекты, стандарты и руководства по основам аудита информационной безопасности;
- основные требования к содержанию аудита защищенности объектов информатизации;
- основы контроля и проверки процессов и систем;
- технологии аудита защищенности объектов информатизации;
- направления обеспечения и оценки информационной безопасности;

### **уметь**

- использовать правовые аспекты, стандарты и руководства по основам аудита защищенности объектов информатизации;
- оценивать защищенность объектов информатизации на основе показателей информационной безопасности;
- исследовать полученные оценки защищенности объектов информатизации;

### **владеть**

- навыками использования методологии, стандартов и нормативных требований в области аудита защищенности объектов информатизации;
- навыками разработки и исследования процессов защиты информации и ее компонентов по результатам аудита защищенности объектов информатизации;

освоить компетенции:

- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3);
- способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

- способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);
- способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

### 3. Место дисциплины в структуре ОП ВО

Дисциплина «Аудит защищенности объектов информатизации» относится к циклу дисциплин по выбору. Дисциплина формирует представление технологиях, применяемых при проведении аудита защищенности объектов информатизации.

Дисциплина изучается на третьем курсе, требования к входным знаниям, умениям и навыкам определяются требованиями к уровню подготовки по дисциплине «Информатика», «Электротехника», «Электроника и схемотехника», «Аппаратные средства вычислительной техники».

Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Основы управления информационной безопасностью», «Комплексные системы защиты информации на предприятии», «Организация системы обеспечения информационной безопасности», «Производственная практика».

### 4. Объем дисциплины (модуля)

#### 4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

| Виды учебной работы,                     | Очная форма     |
|--|-----------------|
| Общая трудоемкость в зачетных единицах   | 3               |
| Общая трудоемкость в часах               | 108             |
| Аудиторные занятия в часах, в том числе: | 50              |
| Лекции                                   | 16              |
| Практические занятия                     | -               |
| Лабораторные занятия                     | 34              |
| Самостоятельная работа в часах           | 58              |
| Форма промежуточной аттестации           | Зачет 6 семестр |

#### 4.2. Объем контактной работы на 1 обучающегося

| Виды учебных занятий | Очная форма |
|----------------------|-------------|
| Лекции               | 16          |
| Практические занятия | -           |
| Лабораторные занятий | 34          |
| Консультации         | 0,8         |
| Зачет/зачеты         | 0,25        |
| Экзамен/экзамены     | -           |
| Курсовые работы      | -           |
| Курсовые проекты     | -           |
| Всего                | 51,05       |

**5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий**

**5.1 Тематический план учебной дисциплины**

| № п/п         | Название раздела, темы  | Всего з.е/час | Аудиторные занятия |              | Самостоятельная работа |
|---------------|---|---------------|--------------------|--------------|------------------------|
|               |   |               | Лекции             | Лабораторные |                        |
| 1.            | Введение. Технические каналы утечки информации.                       | 10            | 2                  | 2            | 9                      |
| 2.            | Средства выявления и контроля ТКУИ.                                   | 20            | 4                  | 8            | 9                      |
| 3.            | Общие вопросы обеспечения защищенности информации.                    | 26            | 2                  | 8            | 10                     |
| 4.            | Методы и средства защиты информации от утечки по техническим каналам. | 26            | 4                  | 8            | 10                     |
| 5.            | Выявление и инструментальная оценка ТКУИ.                             | 26            | 4                  | 8            | 10                     |
| 6.            | Зачет   |               |                    |              | 10                     |
| <b>Всего:</b> |   | <b>108</b>    | <b>16</b>          | <b>34</b>    | <b>58</b>              |

**5.2. Содержание:**

**1. Введение. Технические каналы утечки информации.**

Термины и определения. Потенциально возможные (осуществимые), технические каналы утечки информации. Теоретические основы существования типовых технических каналов утечки информации.

**2. Средства выявления и контроля ТКУИ.**

Общие требования к средствам измерения (выявления) ТКУИ. Измерения акустических и вибрационных сигналов. Измерения электрических сигналов. Измерение электрических и магнитных полей. Измерения сигналов за счет ВЧН/ВЧО. Измерение сигналов в ВОЛП. Специализированные средства измерения.

**3. Общие вопросы обеспечения защищенности информации.**

Требования к защите информации. Состав и выполнение работ. Примеры проведения работ.

**4. Методы и средства защиты информации от утечки по техническим каналам.**

Защита речевой информации. Защита информации, обрабатываемой средствами вычислительной техники. Защита информации, передаваемой по ВОЛП.

**5. Выявление и инструментальная оценка ТКУИ.**

Цель специальных исследований. Задачи специальных исследований. Содержание специальных исследований. Лаборатория проведения специальных исследований. Специальные исследования в области защиты речевой информации. Специальные исследования в области акустоэлектрических преобразований. Специальные исследования в области защиты цифровой информации. Специальные исследования в области ВЧ-навязывания. Специальные исследования в области ВЧ-облучения. Специальные исследования в области защиты ВОЛП.

**6. Методические материалы для обучающихся по освоению дисциплины**

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретиче-

ских ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков применения методов формирования, организации и поддержки комплекса мер по обеспечению информационной безопасности объекта защиты;
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

#### 6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

| № п/п | Раздел (тема) дисциплины | Задание                   | Методические рекомендации по выполнению задания   | Форма контроля    |
|-------|--------------------------|---------------------------|---|-------------------|
| 1     | 2                        | 3                         | 4   | 5                 |
| 1.    | Тема № 1                 | Усвоить                   | 1. Изучить технические каналы утечки информации.<br>Литература основная [1]. Литература дополнительная [1].                                 | Контрольный опрос |
| 2.    | Тема № 2                 | Усвоить, приобрести навык | 1. Изучить средства выявления и контроля ТКУИ.<br>Литература основная [1]. Литература дополнительная [1, 2].                                | Контрольный опрос |
| 3.    | Тема № 3                 | Усвоить, приобрести навык | 1. Изучить общие вопросы обеспечения защищенности информации.<br>Литература основная [1]. Литература дополнительная [1].                    | Контрольный опрос |
| 4.    | Тема № 4                 | Усвоить, приобрести навык | 1. Изучить методы и средства защиты информации от утечки по техническим каналам.<br>Литература основная [1]. Литература дополнительная [1]. | Контрольный опрос |
| 5.    | Тема № 5                 | Усвоить, приобрести навык | 1. Выявить и инструментально оценить ТКУИ.<br>Литература основная [1]. Литература дополнительная [1,2].                                     | Контрольный опрос |

Формой отчетности по данной дисциплине является экзамен. Необходимые условия допуска к экзамену:

- Наличие полного конспекта лекций.
- Сдача всех лабораторных работ с положительным результатом.

**6.2. Тематика и задания для практических занятий (при наличии)**  
*Не предусмотрены*

**6.3. Тематика и задания для лабораторных занятий**

1. Специальные исследования в области защиты речевой информации.
2. Специальные исследования в области акустоэлектрических преобразований.
3. Специальные исследования в области защиты цифровой информации.

**7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)**

**а) основная**

1. Кондратьев А.В. Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки : Справочное пособие. – М. : МАСКОМ, 2011. – 256 с.

**б) дополнительная**

1. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки. Учебное пособие - М: Горячая линия, 2016. - 304 с.
2. Алексеев Д.С. Проведение специальных исследований по каналу ПЭМИН монитора (VGA интерфейса) с использованием ПАК «Сигурд» : учеб. пособие / Д.С. Алексеев, О. В. Щекочихин, А. А. Волков. – Кострома : Изд-во Костром. гос. ун-та, 2018. – 87 с.

**8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

Информационно-образовательные ресурсы:

1. [www.atlas.Krasnodar.ru](http://www.atlas.Krasnodar.ru) -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:

1. Университетская библиотека онлайн <http://biblioclub.ru>
2. «Лань» <http://e.lanbook.com/>
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6. Электронно-библиотечная система (ЭБС) «Инфра-М».
7. Ирисы Фишера  
[http://ru.wikipedia.org/wiki/%C8%F0%E8%F1%FB\\_%D4%E8%F8%E5%F0%E0](http://ru.wikipedia.org/wiki/%C8%F0%E8%F1%FB_%D4%E8%F8%E5%F0%E0)

**9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Лекционная аудитория, оснащенная проектором, компьютером.  
Лаборатория технической защиты информации.