**МИНОБРНАУКИ РОССИИ**
федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Самарский государственный технический университет»**
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ / О.В. Юсупова
"_____" _____ 20___ г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Б1.В.01.08 «Комплексная система защиты информации на предприятии»

| | |
|---|---|
| **Код и направление подготовки (специальность)** | 10.03.01 Информационная безопасность |
| **Направленность (профиль)** | Комплексная защита объектов информатизации (в промышленности) |
| **Квалификация** | Бакалавр |
| **Форма обучения** | Очная |
| **Год начала подготовки** | 2020 |
| **Институт / факультет** | Институт автоматики и информационных технологий |
| **Выпускающая кафедра** | кафедра "Электронные системы и информационная безопасность" |
| **Кафедра-разработчик** | кафедра "Электронные системы и информационная безопасность" |
| **Объем дисциплины, ч. / з.е.** | 144 / 4 |
| **Форма контроля (промежуточная аттестация)** | Экзамен |

Самара 2020

**Б1.В.01.08 «Комплексная система защиты информации на предприятии»**

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **10.03.01 Информационная безопасность**, утвержденного приказом Министерства образования и науки РФ от № 1515 от 01.12.2016 и соответствующего учебного плана.

Разработчик РПД:

| | |
|---|---|
| Доцент, кандидат технических наук | В.Н Ворожейкин |
| (должность, степень, ученое звание) | (ФИО) |

| | |
|---|---|
| Заведующий кафедрой | П.О. Скобелев, доктор технических наук |
| | (ФИО, степень, ученое звание) |

СОГЛАСОВАНО:

| | |
|---|---|
| Председатель методического совета факультета / института (или учебно-методической комиссии) | А.Н Дилигенская, доктор технических наук, доцент |
| | (ФИО, степень, ученое звание) |
| Руководитель образовательной программы | Н.Е. Карпова, кандидат технических наук |
| | (ФИО, степень, ученое звание) |

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы ..... 4
2. Место дисциплины (модуля) в структуре образовательной программы ..... 4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся ..... 5
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий ..... 5
4.1 Содержание лекционных занятий ..... 6
4.2 Содержание лабораторных занятий ..... 7
4.3 Содержание практических занятий ..... 8
4.4. Содержание самостоятельной работы ..... 9
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю) ..... 10
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения ..... 10
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем ..... 10
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) ..... 11
9. Методические материалы ..... 11
10. Фонд оценочных средств по дисциплине (модулю) ..... 13

## 1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| Код и наименование компетенции | Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции) |
|---|---|
| Профессиональные компетенции | |
| ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | Владеть методикой обеспечения комплексной защиты информации В3(ПК-13) — I. |
| | Знать нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. |
| | Знать нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. |
| | Уметь производить обеспечение комплексной защиты информации У3(ПК-13) — I. |
| | Уметь производить обеспечение комплексной защиты информации У3(ПК-13) — I. |
| ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты | Владеть методикой защиты от угроз информационной безопасности В (ПК-4) — I. |
| | Знать общую структуру КСЗИ; угрозы информационной безопасности З (ПК-4) — I. |
| | Уметь выявлять угрозы информационной безопасности У (ПК-4) — I. |
| ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | Владеть методикой защиты от угроз информационной безопасности В (ПК-5) — I. |
| | Знать основы организационно – технических мер ЗИ. З (ПК-5) — I. |
| | Уметь формулировать необходимые организационно – технические меры ЗИ. У (ПК-5) — I. |

## 2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **вариативная часть**

| Код компетенции | Предшествующие дисциплины | Параллельно осваиваемые дисциплины | Последующие дисциплины |
|---|---|---|---|

| | | | |
|---|---|---|---|
| ПК-13 | Методы искусственного интеллекта; Организация и управления службой защиты информации на предприятии; Основы управления информационной безопасностью; Теория и методология защиты информации; Технические средства охраны | Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы | |
| ПК-4 | Производственная практика: эксплуатационная практика | Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы | |
| ПК-5 | Производственная практика: эксплуатационная практика; Техническая защита информации | Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы | |

## 3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

| Вид учебной работы | Всего часов / часов в электронной форме | 8 семестр часов / часов в электронной форме |
|---|---|---|
| **Аудиторная контактная работа (всего),** в том числе: | 72 | 72 |
| Лабораторные работы | 24 | 24 |
| Лекции | 24 | 24 |
| Практические занятия | 24 | 24 |
| **Внеаудиторная контактная работа, КСР** | 4 | 4 |
| **Самостоятельная работа (всего),** в том числе: | 41 | 41 |
| подготовка к лабораторным работам | 21 | 21 |
| подготовка к практическим занятиям | 20 | 20 |
| **Контроль** | 27 | 27 |
| **Итого: час** | 144 | 144 |
| **Итого: з.е.** | 4 | 4 |

## 4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

| № раздела | Наименование раздела дисциплины | Виды учебной нагрузки и их трудоемкость, часы | | | | |
|---|---|---|---|---|---|---|
| | | ЛЗ | ЛР | ПЗ | СРС | Всего часов |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Сущность и структурирование ЗИ предприятия | 12 | 12 | 12 | 21 | 57 |
| 2 | Организация КСЗИ на предприятии | 12 | 12 | 12 | 20 | 56 |
| | **КСР** | 0 | 0 | 0 | 0 | 4 |
| | **Контроль** | 0 | 0 | 0 | 0 | 27 |
| | **Итого** | 24 | 24 | 24 | 41 | 144 |

## 4.1 Содержание лекционных занятий

| **№ занятия** | **Наименование раздела** | **Тема лекции** | **Содержание лекции** (перечень дидактических единиц: рассматриваемых подтем, вопросов) | **Количество часов / часов в электронной форме** |
|---|---|---|---|---|
| **8 семестр** | | | | |
| 1 | Сущность и структурирование ЗИ предприятия | Введение. Сущность и понятие ЗИ предприятия | Предмет, задачи и структура курса. Понятие о ЗИ на предприятии. Состав защищаемой информации предприятия. | 2 |
| 2 | Сущность и структурирование ЗИ предприятия | Введение. Сущность и понятие ЗИ предприятия | Информационные системы предприятий. Структурные уровни автоматизированной информационной системы (АИС). Потребность в комплексной ЗИ, её функции. АИС как объект защиты (для самостоятельного изучения). | 2 |
| 3 | Сущность и структурирование ЗИ предприятия | Анализ угроз информационной безопасности предприятия. Типовые содержания угроз | Задачи оценки информационных угроз АИС. Показатели оценки информационных угроз Содержание угроз информационной безопасности предприятия (для самостоятельного изучения). | 2 |
| 4 | Сущность и структурирование ЗИ предприятия | Анализ угроз информационной безопасности предприятия. Типовые содержания угроз | Выявление множества дестабилизирующих факторов. Формирование их наборов. | 2 |
| 5 | Сущность и структурирование ЗИ предприятия | Структурирование КСЗИ | Понятие о базисах комплексной ЗИ. Основы построения комплексной ЗИ на предприятии. | 2 |
| 6 | Сущность и структурирование ЗИ предприятия | Структурирование КСЗИ | Использование принципов системного подхода (для самостоятельного изучения). Принципы проектирования КСЗИ. | 2 |
| 7 | Организация КСЗИ на предприятии | Политика информационной безопасности. Нормативно – методическое обеспечение ЗИ. | Политика информационной безопасности предприятия. Органы информационной безопасности | 2 |

| | | | | |
|---|---|---|---|---|
| 8 | Организация КСЗИ на предприятии | Политика информационной безопасности. Нормативно – методическое обеспечение ЗИ. | Нормативно – методическое обеспечение ЗИ на предприятии. Правовое обеспечение ЗИ. | 2 |
| 9 | Организация КСЗИ на предприятии | Меры организации комплексной ЗИ на предприятии | Организационно – технические меры ЗИ. Защита делопроизводства. Криптографическая защита. Защита ресурсных объектов АИС. Организация защиты доступа к АИС. (для самостоятельного изучения). | 2 |
| 10 | Организация КСЗИ на предприятии | Меры организации комплексной ЗИ на предприятии | Организация охранно-информационной безопасности служебных объектов. Интеграция подсистем информационной защиты. Рубежи информационной защиты. | 2 |
| 11 | Организация КСЗИ на предприятии | Управление КСЗИ. Заключение | Планирование ЗИ предприятия. Управление КСЗИ предприятия. Группа управления. Обеспечение управляемости КСЗИ (для самостоятельного изучения). | 2 |
| 12 | Организация КСЗИ на предприятии | Управление КСЗИ. Заключение | Оценка эффективности ЗИ. Дальнейшее развитие КСЗИ предприятий | 2 |
| | | | **Итого за семестр:** | **24** |
| | | | **Итого:** | **24** |

## 4.2 Содержание лабораторных занятий

| **№ занятия** | **Наименование раздела** | **Тема лабораторного занятия** | **Содержание лабораторного занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов) | **Количество часов / часов в электронной форме** |
|---|---|---|---|---|
| **8 семестр** | | | | |
| 1 | Сущность и структурирование ЗИ предприятия | Типовые компоненты предприятия, его информационно- управляющей системы. Типовые компоненты подразделения. | Типовые компоненты предприятия, его информационно- управляющей системы. Типовые компоненты подразделения. | 2 |
| 2 | Сущность и структурирование ЗИ предприятия | Типовые компоненты предприятия, его информационно- управляющей системы. Типовые компоненты подразделения. | Типовые компоненты предприятия, его информационно- управляющей системы. Типовые компоненты подразделения. | 2 |
| 3 | Сущность и структурирование ЗИ предприятия | Источники дестабилизирующих воздействий на служебную информацию предприятия. Источники воздействия на служебную информацию подразделения. | Источники дестабилизирующих воздействий на служебную информацию предприятия. Источники воздействия на служебную информацию подразделения. | 2 |
| 4 | Сущность и структурирование ЗИ предприятия | Источники дестабилизирующих воздействий на служебную информацию предприятия. Источники воздействия на служебную информацию подразделения. | Источники дестабилизирующих воздействий на служебную информацию предприятия. Источники воздействия на служебную информацию подразделения. | 2 |

| | | | | |
|---|---|---|---|---|
| 5 | Сущность и структурирование ЗИ предприятия | Признаки нарушения целостности служебной информации предприятия. Организация поиска признаков нарушения целостности. | Признаки нарушения целостности служебной информации предприятия. Организация поиска признаков нарушения целостности. | 2 |
| 6 | Сущность и структурирование ЗИ предприятия | Признаки нарушения целостности служебной информации предприятия. Организация поиска признаков нарушения целостности. | Признаки нарушения целостности служебной информации предприятия. Организация поиска признаков нарушения целостности. | 2 |
| 7 | Организация КСЗИ на предприятии | Реализация избирательной политики информационной безопасности на предприятии. Реализация полномочной политики информационной безопасности на предприятии. | Реализация избирательной политики информационной безопасности на предприятии. Реализация полномочной политики информационной безопасности на предприятии. | 2 |
| 8 | Организация КСЗИ на предприятии | Реализация избирательной политики информационной безопасности на предприятии. Реализация полномочной политики информационной безопасности на предприятии. | Реализация избирательной политики информационной безопасности на предприятии. Реализация полномочной политики информационной безопасности на предприятии. | 2 |
| 9 | Организация КСЗИ на предприятии | Формирование мер информационной безопасности предприятия по рубежам защиты. Защита по территориальным и информационно-вычислительным рубежам. | Формирование мер информационной безопасности предприятия по рубежам защиты. Защита по территориальным и информационно-вычислительным рубежам. | 2 |
| 10 | Организация КСЗИ на предприятии | Формирование мер информационной безопасности предприятия по рубежам защиты. Защита по территориальным и информационно-вычислительным рубежам. | Формирование мер информационной безопасности предприятия по рубежам защиты. Защита по территориальным и информационно-вычислительным рубежам. | 2 |
| 11 | Организация КСЗИ на предприятии | Планирование информационной защиты предприятия. Разработка основных компонентов плана защиты. | Планирование информационной защиты предприятия. Разработка основных компонентов плана защиты. | 2 |
| 12 | Организация КСЗИ на предприятии | Планирование информационной защиты предприятия. Разработка основных компонентов плана защиты. | Планирование информационной защиты предприятия. Разработка основных компонентов плана защиты. | 2 |
| | | | **Итого за семестр:** | **24** |
| | | | **Итого:** | **24** |

## 4.3 Содержание практических занятий

| **№ занятия** | **Наименование раздела** | **Тема практического занятия** | **Содержание практического занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов) | **Количество часов / часов в электронной форме** |
|---|---|---|---|---|
| **8 семестр** | | | | |
| 1 | Сущность и структурирование ЗИ предприятия | Автоматизированная информационная система как объект ЗИ. Единичный объект информзащиты. | Автоматизированная информационная система как объект ЗИ. Единичный объект информзащиты. | 2 |
| 2 | Сущность и структурирование ЗИ предприятия | Автоматизированная информационная система как объект ЗИ. Единичный объект информзащиты. | Автоматизированная информационная система как объект ЗИ. Единичный объект информзащиты. | 2 |

| | | | | |
|---|---|---|---|---|
| 3 | Сущность и структурирование ЗИ предприятия | Задачи и показатели оценки информационных угроз. Содержание угроз информационной безопасности. | Задачи и показатели оценки информационных угроз. Содержание угроз информационной безопасности. | 2 |
| 4 | Сущность и структурирование ЗИ предприятия | Задачи и показатели оценки информационных угроз. Содержание угроз информационной безопасности. | Задачи и показатели оценки информационных угроз. Содержание угроз информационной безопасности. | 2 |
| 5 | Сущность и структурирование ЗИ предприятия | Базовые принципы построения КСЗИ на предприятии. Принципы построения КСЗИ в подразделении. | Базовые принципы построения КСЗИ на предприятии. Принципы построения КСЗИ в подразделении. | 2 |
| 6 | Сущность и структурирование ЗИ предприятия | Базовые принципы построения КСЗИ на предприятии. Принципы построения КСЗИ в подразделении. | Базовые принципы построения КСЗИ на предприятии. Принципы построения КСЗИ в подразделении. | 2 |
| 7 | Организация КСЗИ на предприятии | Организационные мероприятия по ЗИ на предприятии.Подход к выработке мероприятий по ЗИ. | Организационные мероприятия по ЗИ на предприятии.Подход к выработке мероприятий по ЗИ. | 2 |
| 8 | Организация КСЗИ на предприятии | Организационные мероприятия по ЗИ на предприятии.Подход к выработке мероприятий по ЗИ. | Организационные мероприятия по ЗИ на предприятии.Подход к выработке мероприятий по ЗИ. | 2 |
| 9 | Организация КСЗИ на предприятии | Организационно-технические меры по ЗИ. Административные аспекты мер ЗИ. | Организационно-технические меры по ЗИ. Административные аспекты мер ЗИ. | 2 |
| 10 | Организация КСЗИ на предприятии | Организационно-технические меры по ЗИ. Административные аспекты мер ЗИ. | Организационно-технические меры по ЗИ. Административные аспекты мер ЗИ. | 2 |
| 11 | Организация КСЗИ на предприятии | Управление комплексной ЗИ предприятия. Комплексное управление ЗИ в подразделении. | Управление комплексной ЗИ предприятия. Комплексное управление ЗИ в подразделении. | 2 |
| 12 | Организация КСЗИ на предприятии | Управление комплексной ЗИ предприятия. Комплексное управление ЗИ в подразделении. | Управление комплексной ЗИ предприятия. Комплексное управление ЗИ в подразделении. | 2 |
| | | | **Итого за семестр:** | **24** |
| | | | **Итого:** | **24** |

## 4.4. Содержание самостоятельной работы

| **Наименование раздела** | **Вид самостоятельной работы** | **Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов) | **Количество часов** |
|---|---|---|---|
| **8 семестр** | | | |
| Сущность и структурирование ЗИ предприятия | Подготовка к лабораторным работам | - | 21 |

| | | | |
|---|---|---|---|
| Организация КСЗИ на предприятии | Подготовка к практическим занятиям | - | 20 |
| | | **Итого за семестр:** | **41** |
| | | **Итого:** | **41** |

## 5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

| **№ п/п** | **Библиографическое описание** | **Ресурс НТБ СамГТУ** (ЭБС СамГТУ, IPRbooks и т.д.) |
|---|---|---|
| Основная литература | | |
| 1 | Галатенко, В.А. Стандарты информационной безопасности : Курс лекций / Под ред.В.Б.Бетелина.- М., Интернет-Ун-т Информ.Технологий, 2004.- 326 с. | Электронный ресурс |
| 2 | Основы информационной безопасности; Санкт-Петербургский политехнический университет Петра Великого, 2014.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu\|\|iprbooks\|\|43960 | Электронный ресурс |

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

## 6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

| **№ п/п** | **Наименование** | **Производитель** | **Способ распространения** |
|---|---|---|---|
| 1 | ASTRA LINUX | ГК ASTRA LINUX (Отечественный) | Лицензионное |
| 2 | Windows 10 | Microsoft (Зарубежный) | Лицензионное |

## 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

| **№ п/п** | **Наименование** | **Краткое описание** | **Режим доступа** |
|---|---|---|---|
| 1 | РОСПАТЕНТ | http://www1.fips.ru/wps/wcm/connect/content_ru/ru | Ресурсы открытого доступа |
| 2 | Консультатнт плюс | http://www.consultant.ru/ | Ресурсы открытого доступа |

## 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

**Лекционные занятия**

**1. Лекционные занятия:**

Аудитория, оборудованная учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска.

**Практические занятия**

**2. Практические занятия:**

компьютерный класс на 10 посадочных мест (ауд. 109, 8 корпус), оснащенный компьютерами Pentium IV 3,0 ГГц / 1 Gb / 160 Gb / DVD-RW с мониторами Lg L1752S TFT 17" - 10 шт.

**Лабораторные занятия**

3. Лабораторные занятия:

компьютерный класс на 10 посадочных мест (ауд. 109, 8 корпус), оснащенный компьютерами Pentium IV 3,0 ГГц / 1 Gb / 160 Gb / DVD-RW с мониторами Lg L1752S TFT 17" - 10 шт.

**Самостоятельная работа**

**4 . Прочее:**

Для самостоятельной работы обучающихся предусмотрены рабочие места в читальных залах научно-технической библиотеки и компьютерных классах, ресурсы информационно-вычислительного центра ФГБОУ ВО «СамГТУ», оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной информационной среде.

## 9. Методические материалы

### Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно

значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

## Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

## Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и

индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимися выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчётности по данной работе.

## Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

## 10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.01.08 «Комплексная система защиты информации на предприятии»

**Фонд оценочных средств**
**по дисциплине**
**Б1.В.01.08 «Комплексная система защиты информации на предприятии»**

| | |
|---|---|
| **Код и направление подготовки (специальность)** | 10.03.01 Информационная безопасность |
| **Направленность (профиль)** | Комплексная защита объектов информатизации (в промышленности) |
| **Квалификация** | Бакалавр |
| **Форма обучения** | Очная |
| **Год начала подготовки** | 2020 |
| **Институт / факультет** | Институт автоматики и информационных технологий |
| **Выпускающая кафедра** | кафедра "Электронные системы и информационная безопасность" |
| **Кафедра-разработчик** | кафедра "Электронные системы и информационная безопасность" |
| **Объем дисциплины, ч. / з.е.** | 144 / 4 |
| **Форма контроля (промежуточная аттестация)** | Экзамен |

## Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| Код и наименование компетенции | Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции) |
|---|---|
| Профессиональные компетенции | |
| ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | Владеть методикой обеспечения комплексной защиты информации В3(ПК-13) — I. |
| | Знать нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. |
| | Знать нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. |
| | Уметь производить обеспечение комплексной защиты информации У3(ПК-13) — I. |
| | Уметь производить обеспечение комплексной защиты информации У3(ПК-13) — I. |
| ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты | Владеть методикой защиты от угроз информационной безопасности В (ПК-4) — I. |
| | Знать общую структуру КСЗИ; угрозы информационной безопасности З (ПК-4) — I. |
| | Уметь выявлять угрозы информационной безопасности У (ПК-4) — I. |
| ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | Владеть методикой защиты от угроз информационной безопасности В (ПК-5) — I. |
| | Знать основы организационно – технических мер ЗИ. З (ПК-5) — I. |
| | Уметь формулировать необходимые организационно – технические меры ЗИ. У (ПК-5) — I. |

## Матрица соответствия оценочных средств запланированным результатам обучения

| Код и наименование компетенции | Результаты обучения | Оценочные средства | Текущий контроль успеваемости | Промежуточная аттестация |
|---|---|---|---|---|
| **Сущность и структурирование ЗИ предприятия** | | | | |

| | | | | |
|---|---|---|---|---|
| ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | **Знать** нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. | Собеседование | Да | Да |
| | **Владеть** методикой обеспечения комплексной защиты информации В3(ПК-13) — I. | Собеседование | Да | Да |
| | **Знать** нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. | Собеседование | Да | Да |
| | **Уметь** производить обеспечение комплексной защиты информации У3(ПК-13) — I. | Собеседование | Да | Да |
| | **Уметь** производить обеспечение комплексной защиты информации У3(ПК-13) — I. | Собеседование | Да | Да |
| ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты | **Уметь** выявлять угрозы информационной безопасности У (ПК-4) — I. | Собеседование | Да | Да |
| | **Владеть** методикой защиты от угроз информационной безопасности В (ПК-4) — I. | Собеседование | Да | Да |
| | **Знать** общую структуру КСЗИ; угрозы информационной безопасности З (ПК-4) — I. | Собеседование | Да | Да |
| ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | **Знать** основы организационно – технических мер ЗИ. З (ПК-5) — I. | Собеседование | Да | Да |
| | **Владеть** методикой защиты от угроз информационной безопасности В (ПК-5) — I. | Собеседование | Да | Да |
| | **Уметь** формулировать необходимые организационно – технические меры ЗИ. У (ПК-5) — I. | Собеседование | Да | Да |
| **Организация КСЗИ на предприятии** | | | | |

| | | | | |
|---|---|---|---|---|
| ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации | **Владеть** методикой обеспечения комплексной защиты информации В3(ПК-13) — I. | Собеседование | Да | Да |
| | **Знать** нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. | Собеседование | Да | Да |
| | **Знать** нормативно-методическое обеспечение защиты информации З3(ПК-13) — I. | Собеседование | Да | Да |
| | **Уметь** производить обеспечение комплексной защиты информации У3(ПК-13) — I. | Собеседование | Да | Да |
| | **Уметь** производить обеспечение комплексной защиты информации У3(ПК-13) — I. | Собеседование | Да | Да |
| ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты | **Уметь** выявлять угрозы информационной безопасности У (ПК-4) — I. | Собеседование | Да | Да |
| | **Знать** общую структуру КСЗИ; угрозы информационной безопасности З (ПК-4) — I. | Собеседование | Да | Да |
| | **Владеть** методикой защиты от угроз информационной безопасности В (ПК-4) — I. | Собеседование | Да | Да |
| ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | **Владеть** методикой защиты от угроз информационной безопасности В (ПК-5) — I. | Собеседование | Да | Да |
| | **Знать** основы организационно – технических мер ЗИ. З (ПК-5) — I. | Собеседование | Да | Да |
| | **Уметь** формулировать необходимые организационно – технические меры ЗИ. У (ПК-5) — I. | Собеседование | Да | Да |

## Список вопросов для промежуточного контроля (экзамен)

1. Понятие о комплексной системе защиты информации на предприятии.
2. Автоматизированные информационные системы предприятий.
3. Состав защищаемой служебной информации.
4. Потребности в функциях и компонентах информационно – защитных систем.
5. АИС как объект информационной защиты.
6. Задачи оценки и содержание показателей информационной уязвимости .
7. Параметры влияния на рост информационных нарушений, комбинации показателей информационных угроз.
8. Содержание угроз информационной безопасности предприятия.
9. Формирование перечня дестабилизирующих факторов, влияющих на АИС предприятия.
10. Принципы построения систем защиты информации предприятий.
11. Требования к разработке нормативной документации по информационной защите предприятия.
12. Базисы комплексной защиты информации предприятия.
13. Структуры систем безопасности и информационной безопасности предприятия.
14. Условия проектирования системы информационной защиты, подход к проектированию.
15. Последовательность этапов проектирования системы информационной защиты.
16. Понятие о базисах комплексной информационной защиты.
17. Использование принципов системного подхода в деле защиты информации.
18. Принципы проектирования комплексных систем защиты информации.
19. Избирательная политика информационной безопасности.
20. Полномочная политика информационной безопасности.
21. Общие процедуры обеспечения сохранности служебной информации.
22. Организационно – административные меры информационной защиты на предприятии.
23. Организационно – технические мероприятия по информационной защите предприятия.
24. Организация защищенного делопроизводства на предприятии.
25. Методические основы проверки пользователей АИС.
26. Методические основы проверки адресатов информационной передачи.
27. Организация защиты ресурсов АИС предприятия.

28. Организация мер противодействия вторжениям в процессы информационной передачи.

29. Организация мер защиты при пересылке электронных документов.

30. Организация информационной безопасности объектов инфраструктуры предприятия.

31. Организация криптографической защиты на предприятии.

32. Комплексирование информационно – защитных мер на предприятии.

33. Комплексирование подсистем информационной защиты.

34. Комплексирование средств защиты информации на предприятии.

35. Понятие об управлении информационной защитой на предприятии.

36. Группа управления информационной защитой на предприятии.

37. Комплексирование средств защиты и средств управления защитой.

38. Принципы контроля и реализации политики информационной безопасности предприятия.

39. Функции и характер управления защитой информации на предприятии.

40. Комплексное управление доступом к информации и информационными потоками.

41. Оценка эффективности информационно – защитных мероприятий.

42. Обследование предприятия по обеспеченности информационной защиты.

43. Понятие о типизации средств информационной защиты предприятия.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Электронные системы и информационная безопасность»

по дисциплине **Комплексная система защиты информации на предприятии**

(наименование дисциплины)

| | | | | | |
|---|---|---|---|---|---|
| Направление подготовки | **10.03.01** | Факультет | АИТ | Семестр | **8** |
| | (шифр) | | (наименование факультета) | | (номер) |

# БИЛЕТ № 1

1. Понятие о комплексной системе защиты информации предприятия
2. Организация защищенного делопроизводства на предприятии

Составитель:

_____ профессор Никонов А.И.

«____» _____ 20__ года

Заведующий кафедрой

_____ Скобелев П.О.

«____» _____ 20__ года

## Список вопросов для промежуточного контроля (экзамен)

1. Понятие о комплексной системе защиты информации на предприятии.
2. Автоматизированные информационные системы предприятий.
3. Состав защищаемой служебной информации.
4. Потребности в функциях и компонентах информационно – защитных систем.
5. АИС как объект информационной защиты.
6. Задачи оценки и содержание показателей информационной уязвимости .
7. Параметры влияния на рост информационных нарушений, комбинации показателей информационных угроз.
8. Содержание угроз информационной безопасности предприятия.
9. Формирование перечня дестабилизирующих факторов, влияющих на АИС предприятия.
10. Принципы построения систем защиты информации предприятий.
11. Требования к разработке нормативной документации по информационной защите предприятия.
12. Базисы комплексной защиты информации предприятия.
13. Структуры систем безопасности и информационной безопасности предприятия.
14. Условия проектирования системы информационной защиты, подход к проектированию.
15. Последовательность этапов проектирования системы информационной защиты.
16. Понятие о базисах комплексной информационной защиты.
17. Использование принципов системного подхода в деле защиты информации.
18. Принципы проектирования комплексных систем защиты информации.
19. Избирательная политика информационной безопасности.
20. Полномочная политика информационной безопасности.
21. Общие процедуры обеспечения сохранности служебной информации.
22. Организационно – административные меры информационной защиты на предприятии.
23. Организационно – технические мероприятия по информационной защите предприятия.
24. Организация защищенного делопроизводства на предприятии.
25. Методические основы проверки пользователей АИС.
26. Методические основы проверки адресатов информационной передачи.
27. Организация защиты ресурсов АИС предприятия.

28. Организация мер противодействия вторжениям в процессы информационной передачи.

29. Организация мер защиты при пересылке электронных документов.

30. Организация информационной безопасности объектов инфраструктуры предприятия.

31. Организация криптографической защиты на предприятии.

32. Комплексирование информационно – защитных мер на предприятии.

33. Комплексирование подсистем информационной защиты.

34. Комплексирование средств защиты информации на предприятии.

35. Понятие об управлении информационной защитой на предприятии.

36. Группа управления информационной защитой на предприятии.

37. Комплексирование средств защиты и средств управления защитой.

38. Принципы контроля и реализации политики информационной безопасности предприятия.

39. Функции и характер управления защитой информации на предприятии.

40. Комплексное управление доступом к информации и информационными потоками.

41. Оценка эффективности информационно – защитных мероприятий.

42. Обследование предприятия по обеспеченности информационной защиты.

43. Понятие о типизации средств информационной защиты предприятия.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Электронные системы и информационная безопасность»

по дисциплине **Комплексная система защиты информации на предприятии**

(наименование дисциплины)

| | | | | | |
|---|---|---|---|---|---|
| Направление подготовки | **10.03.01** | Факультет | АИТ | Семестр | **8** |
| | (шифр) | | (наименование факультета) | | (номер) |

# БИЛЕТ № 1

1. Понятие о комплексной системе защиты информации предприятия
2. Организация защищенного делопроизводства на предприятии

Составитель:

_____ профессор Никонов А.И.

«____» _____ 20__ года

Заведующий кафедрой

_____ Скобелев П.О.

«____» _____ 20__ года