ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование
дисциплины (модуля): **Управление информационной безопасностью**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Какорина О. А., кандидат физико-математических наук, заведующий кафедрой

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, эксплуатации и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

Задачи дисциплины:

- формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем
- ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем
- обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Управление информационной безопасностью» относится к обязательной части учебного плана.

Дисциплина изучается на 4 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- ОПК-4.3 Способен разрабатывать и анализировать корректность политики информационной
безопасности компьютерных систем и сетей (по областям применения)

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

последовательность и содержание этапов построения компьютерных сетей; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; типовые структуры и принципы организации компьютерных сетей; примеры реализации современных локальных и глобальных компьютерных сетей; основные телекоммуникационные протоколы; перспективы развития компьютерных сетей

Студент должен уметь:

анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем

Студент должен владеть навыками:

навыками разработки технических заданий на создание средств защиты информации; в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

- ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

основные нормативные правовые акты в области информационной безопасности и защиты информации, нормативные и методические документы Федеральной службы безопасности по техническому и экспортному контролю в данной области

Студент должен уметь:

применять нормативные правовые акты в своей профессиональной деятельности

Студент должен владеть навыками:

навыками работы с нормативными правовыми актами

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Седьмой семестр
Контактная работа (всего)	**84**	**84**
Лабораторные	34	34
Лекции	34	34
Практические	16	16
Самостоятельная работа (всего)	**60**	**60**
Виды промежуточной аттестации		
Зачет с оценкой		+
Общая трудоемкость часы	**144**	**144**
Общая трудоемкость зачетные единицы	**4**	**4**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лекции (34 ч.)

Седьмой семестр. (34 ч.)

Тема 1. Сущность и функции управления. (2 ч.)

Сущность и функции управления. Принципы, подходы и методология управления. Цели и задачи управления ИБ. Понятие системы управления

Тема 2. Понятие процесса. (2 ч.)

Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации,
эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Модель PDCA

Тема 3. Стандартизация в области построения систем управления. (2 ч.)

Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ.

Тема 4. Система управления информационной безопасностью (СУИБ) (2 ч.)

Система управления информационной безопасностью (СУИБ)
Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ
Этапы разработки и функционирования СУИБ

Тема 5. Политика СУИБ. (2 ч.)

Политика СУИБ.
Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ. Понятие и виды защищаемой информации по законодательству РФ. Примеры политики СУИБ

Тема 6. Цель процесса анализа рисков ИБ. (2 ч.)

Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах

организации. Основные положения стандартов в области управления рисками ИБ.

Тема 7. Цель процесса анализа рисков ИБ. (2 ч.)

Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Основные положения стандартов в области управления рисками ИБ.

Тема 8. Угрозы ИБ. (2 ч.)

Угрозы ИБ. Основные источники угроз. Понятие уязвимостей. Классификация угроз. Модель угроз. Методы оценки ущерба от реализации угроз информационной безопасности

Тема 9. Методики анализа рисков ИБ. (2 ч.)

Методики анализа рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Использование результатов анализа рисков ИБ.

Тема 10. Методики анализа рисков ИБ. (2 ч.)

Методики анализа рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Использование результатов анализа рисков ИБ.

Тема 11. Мониторинг защищенности и аудит ИБ. (2 ч.)

Мониторинг состояния защищенности информации. Самооценка организации управления ИБ. Организация и проведение аудита ИБ. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация.

Тема 12. Ввод системы в эксплуатацию. (2 ч.)

Ввод системы в эксплуатацию.

Тема 13. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. (2 ч.)

Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

Тема 14. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. (2 ч.)

Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

Тема 15. Анализ функционирования СУИБ (2 ч.)

Оценка эффективности СУИБ. Виды. Результативность СУИБ.

Тема 16. Этапы внедрения процессов и их последовательность. (2 ч.)

Этапы внедрения процессов и их последовательность. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости».

Тема 17. Этапы внедрения процессов и их последовательность. (2 ч.)

Этапы внедрения процессов и их последовательность.
Контроль над внедрением процессов.
Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости».

5.2. Содержание дисциплины: Практические (16 ч.)

Седьмой семестр. (16 ч.)

Тема 1. Системный подход к управления организацией (2 ч.)

Ознакомиться с терминологией и методическими принципами системного подхода.

Тема 2. Процессный подход к управлению организацией (2 ч.)

Ознакомиться с терминологией и методологическими принципами процессного подхода.

Тема 3. Стандартизация в области построения систем управления. (2 ч.)

Изучение серии стандартов по управлению ИБ.

Тема 4. Методика анализа рисков информационной безопасности (2 ч.)

Изучение методики анализа рисков ИБ. Этапы процесса управления рисками ИБ.

Тема 5. Методы анализа бизнес-процессов (2 ч.)

Изучение методов декомпозиции, методологий структурного анализа - теории ИСМ, методологии IDEF0, объектно-ориентированной методологии.

Тема 6. Формирование и анализ иерархии целей управления ИБ (2 ч.)

Выявление основных целей управления ИБ. Построение дерева целей.

Тема 7. Сравнительный анализ моделей организационного управления ИБ (2 ч.)

Базовые модели организационного управления ИБ. Достоинства и недостатки каждого типа управления.

Тема 8. Угрозы ИБ. (2 ч.)

Угрозы ИБ. Основные источники угроз. Понятие уязвимостей. Классификация угроз. Модель угроз. Методы оценки ущерба от реализации угроз информационной безопасности

5.3. Содержание дисциплины: Лабораторные (34 ч.)

Седьмой семестр. (34 ч.)

Тема 1. Этап «Планирование» процедур СОИБ. Планирование работ по разработке Политики организации (2 ч.)

Описание объекта защиты; проведение анализа рисков; формирование перечня критичных ресурсов; определение модели нарушителя; определение модели угроз информационной безопасности; определение перечня требований информационной безопасности ИС; разработка комплекса организационных и программно-технических мер по реализации требований ИБ ИС и построению подсистемы информационной безопасности ИС; разработка организационно-технической схемы контроля состояния информационной безопасности ИС.

Тема 2. Планирование работ по созданию СИБ в соответствии с требованиями Политики организации (2 ч.)

Разработка и утверждение технического задания на создание СИБ в соответствии с ГОСТ 34.601-9.

Тема 3. Анализ рисков в ИС. Обработка рисков (2 ч.)

Идентификация и определение ценности всех активов в рамках выбранной области деятельности; оценка защищенности ИС; оценка рисков в отношении ценных активов. Выбор способа обработки рисков; подготовка плана обработки рисков или плана мероприятий по снижению рисков с указанием контрмер (административные, организационные, программно-технические); расчет эффективности выбранных контрмер по снижению рисков.

Тема 4. Планирование системы мониторинга ИБ и защитных мер СОИБ (2 ч.)

Системы мониторинга ИБ. Планирование основных принципов построения ЕСМИБ.

Тема 5. Планирование проведения аудита ИБ организации. (2 ч.)

Разработка типовой программы аудитов ИБ, содержащую информацию, необходимую для планирования и организации аудита ИБ, анализа исовершенствования СУИБ. Подгтовка отчетов по результатам проведения аудита ИБ.

Тема 6. Этап «Реализация» процедур СОИБ. Выполнение работ по внедрению СИБ организации (2 ч.)

Определение класса защищенности ИС. Выбор защитных мер и механизмов защиты для построения СИБ соответствеющего класса защищенности ИС.

Тема 7. Внедрение системы управления рисками (2 ч.)

Выбор анализируемых объектов и уровня детализации их рассмотрения; выбор методики оценки рисков; инвентаризация активов; анализ угроз и их последствий, выявление уязвимых мест взащите; оценка рисков; обработка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска.

Тема 8. Внедрение системы управления инцидентами ИБ (2 ч.)

Разработать необходимые нормативные документы по управлению инцидентами (определение инцидента ИБ; методику регистрации инцидента ИБ; порядок оповещения ответственных лиц овозникновении инцидента ИБ; порядок устранения последствий и причин инцидента ИБ; порядок расследования инцидента ИБ; внесение дисциплинарных взысканий; реализация необходимых корректирующих и превентивных мер и др.).

Тема 9. Внедрение систем мониторинга ИБ и контроля защитных мер СОИБ (2 ч.)

Обзор рынка систем интегрального мониторинга ИБ зарубежного и отечественного производства. Выбор системы мониторинга.

Тема 10. Внедрение системы самооценки и аудита ИБ организации. (2 ч.)

Разработать внутреннюю методику самооценки состояния ИБ. Разработать программу аудита ИБ организации. Оформить план аудита.

Тема 11. Ввод в эксплуатацию СУИБ (2 ч.)

Разработать: план внедрения системы управления, инструкцию по обеспечению сохранности конфиденциальной информации, инструкцию пользователя по обеспечению ИБ, инструкцию системного администратора по обеспечению ИБ, инструкция администратора безопасности, инструкцию по выполнению резервного копирования, инструкцию по обращению со съемными носителями информации, инструкцию по использованию средств криптографической защиты информации.

Тема 12. Этап «Проверка» СОИБ. Проверка результатов мониторинга ИБ и контроля защитных мер СОИБ (2 ч.)

Проверка организационно-технической схемы применения ЕСМИБ. Ппроверка реализации положений внутренних документов пообеспечению ИБ в организации и требований нормативных документов по ИБ РФ. Оформить результаты проверки оперативного мониторинга ИБ и контроля защитных мер СОИБ.

Тема 13. Проверка результатов проведения самооценки и аудита ИБ организации (2 ч.)

Разработать внутреннюю методику самооценки состояния ИБ. Разработать программу аудита ИБ организации. Оформить план аудита.

Тема 14. Этап «Совершенствование» СОИБ. (2 ч.)

Оценка новых угроз и уязвимостей ИБ.

Тема 15. Анализ оценок функционирования СОИБ со стороны руководства (2 ч.)

Проведение анализа оценки функционирования СОИБ на основании: отчета с результатами мониторинга ИБ и контроля защитных мер; отчета с результатами анализа функционирования СОИБ; отчета с результатами аудитов ИБ; отчета с результатами самооценок ИБ; документов, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ и т.п.

Тема 16. Актуализация базы данных изменений в законодательстве (2 ч.)

Актуализация базы данных изменений в законодательстве Российской Федерации и нормативных актах организации, целях и задачах бизнеса.

Тема 17. Совершенствование СОИБ в виде корректирующих или превентивных действий (2 ч.)

Разработать план реализации тактических и стратегических улучшений СОИБ, и документы, в которых фиксируются результаты выполнения указанных планов. Направления тактических и стратегических улучшений СОИБ в виде корректирующих и превентивных действий: уточнение/пересмотр целей и задач обеспечения ИБ, определенных в политике ИБ; изменение в области действия СОИБ; уточнение описи типов информационных активов; пересмотр моделей угроз и нарушителей; пересмотр процедур обнаружения и обработки инцидентов; пересмотр программы обучения и повышения осведомленности персонала; пересмотр планов обработки рисков; пересмотр процедур мониторинга СОИБ и контроля защитных мер; пересмотр программ аудитов; корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер; ввод новых или замена используемых защитных мер.

6. Виды самостоятельной работы студентов по дисциплине

Седьмой семестр (60 ч.)

Вид СРС: Ознакомление с нормативными документами (60 ч.)

Тематика заданий СРС:

Ознакомление с нормативными документами:

1. ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология;
2. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
3. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Сводноpм и правил применения мер обеспечения информационнойбезопасности;
4. ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство пореализации;
5. ГОСТ Р ИСО/МЭК 27004-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание;
6. ГОСТ Р ИСО/МЭК 27005-2010 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности;
7. ГОСТ Р ИСО/МЭК 27006-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Требования корганам, осуществляющим аудит и сертификацию систем ме-неджмента информационной безопасности;
8. ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности;
9. ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011 «СМИБ. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью;
10. ГОСТ Р ИСО/МЭК 27010-2020 «Информационные технологии. Методы и средства обеспечения безопасности при обмене информацией между отраслями и организациями;
11. ГОСТ Р ИСО/МЭК 27017-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности наоснове ИСО/МЭК 27002 при использовании облачных служб;
12. ГОСТ Р ИСО/МЭК 27018-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных в публичных облаках,используемых для их обработки.
13. ГОСТ Р ИСО/МЭК 27019-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной);
14. ГОСТ Р ИСО/МЭК 27021-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности.

Стандарт «Критерии оценки доверенных компьютерных систем» (Оранжевая книга);
3. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
4. Рекомендации Х.800, «Архитектура безопасности для взаимодействия открытых систем»;
5. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информациооной безопасностью

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более
Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.
Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Студент должен знать:

основные нормативные правовые акты в области информационной безопасности и защиты информации, нормативные и методические документы Федеральной службы безопасности по техническому и экспортному контролю в данной области

Вопросы, задания:

1. Стандарт ISO/IEC 17799.
2. ГОСТ Р ИСО/МЭК 27001.

3. Основные нормативные правовые акты по защите информации в РФ.

Студент должен уметь:

применять нормативные правовые акты в своей профессиональной деятельности

Задания:

1. Классификация государственных информационных систем по требованиям защиты информации.

2. Определение мер защиты информации в государственной информационной системе.

3. Определить угрозы безопасности информации.

Студент должен владеть навыками:

навыками работы с нормативными правовыми актами

Задания:

1. Провести анализ нормативных правовых актов, методических документов, которым должна соответствовать государственная информационная система.

2. Определить ребования к системе защиты информации государственной информационной системы.

3. Разработать систему защиты информации государственной информационной системы.

- ОПК-4.3 Способен разрабатывать и анализировать корректность политики информационной
безопасности компьютерных систем и сетей (по областям применения)

Студент должен знать:

последовательность и содержание этапов построения компьютерных сетей; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; типовые структуры и принципы организации компьютерных сетей; примеры реализации современных локальных и глобальных компьютерных сетей; основные телекоммуникационные протоколы; перспективы развития компьютерных сетей

Вопросы, задания:

1. Этапы разработки и функционирования СУИБ.

2. Структура и содержание Политики СУИБ.

3. СУИБ понятие и основные функции.

Студент должен уметь:

анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем

Задания:

1. Постоить модель угроз выбранной организации.

2. Разработать модель нарушителя выбранной организации.

3. Разработать частную политику безопасности выбранной организации.

Студент должен владеть навыками:

навыками разработки технических заданий на создание средств защиты информации; в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

Задания:

1. Принципы управления информационной безопасностью
2. Разработать политику информационной безопасности предприятия.
3. Определить класс защищенности ИС.

8.3. Вопросы промежуточной аттестации

Седьмой семестр (Зачет с оценкой)

1. Сущность и функции управления.
2. Принципы, подходы и методология управления.
3. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов.
4. Понятие процессного подхода. Модель PDCA.
5. Существующие стандарты и методологии по управлению ИБ.
6. Понятие СУИБ. Область деятельности СУИБ. Этапы разработки и функционирования СУИБ.
7. Политика СУИБ. Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ.
8. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ.
9. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах
10. Угрозы ИБ. Классификация угроз. Модель угроз. Методы оценки ущерба от реализации угроз информационной безопасности.
11. Методики анализа рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Использование результатов анализа рисков ИБ.
12. Ввод системы в эксплуатацию. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация.

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Зачет с оценкой

зачет с оценкой служит формой проверки усвоения учебного материала по дисциплине (модулю), практики, готовности к практической деятельности.

Методика формирования результирующей оценки:

Седьмой семестр

1. Контрольная работа - от 0 до 30 баллов

2. Устный опрос, собеседование - от 0 до 20 баллов

3. Письменные задания или лабораторные работы - от 0 до 60 баллов

4. Зачет с оценкой - Аттестация по дисциплине в форме зачета (зачета с оценкой) проводится по сумме результатов модульных контрольных работ и текущей успеваемости обучающегося.

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. И. В. Капгер, А. С. Шабуров Управление информационной безопасностью : учебное пособие [Электронный ресурс]: - Пермь : ПНИПУ, 2023. - 91 с.

2. Мошак, Н. Н. Основы управления информационной безопасностью : учебное пособие [Электронный ресурс]: - Санкт-Петербург : ГУАП, 2022. - 141 с. - Режим доступа: https://e.lanbook.com/book/340967

9.2 Дополнительная литература

1. Н. Г. Милославская, А. И. Толстой. Управление информационной безопасностью: Конспект лекций : учебное пособие [Электронный ресурс]: - Москва : НИЯУ МИФИ, 2020. - 536 с. - Режим доступа: https://e.lanbook.com/book/284378

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru - Научная электронная библиотека

2. http://ibooks.ru/ - Электронная библиотечная система учебной и научной литературы

3. http://www.edu.ru. - Федеральный портал «Российское образование»

4. https://biblio-online.ru/ - Электронная библиотека

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:

- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Лицензионное программное обеспечение:
1. Oracle VM VirtualBox 10 лицензий GNU GPL свободное программное обеспечение;
2. FreeBSD, 10 лицензий FreeBSD license свободное программное обеспечение;
3. Microsoft Windows 7 Home Premium, 2 OEM-лицензии;
4. Microsoft Windows 8.1 Home, 1 OEM-лицензия;
5. 7-zip, 3 лицензии GNU LGPL свободное программное обеспечение;
6. Microsoft Office 2007 Standart, 2 лицензии, номер 43847745;
7. Антивирус Kaspersky Endpoint Security, 3 лицензии, номер 500999;
8. Mozila FireFox Mozilla Public License 2.0 (MPL), 3 лицензии, свободное программное обеспечение;
9. Visual Studio Community 2017, 13 лицензий, учебное программное обеспечение;
10. Microsoft Windows 7 – лицензия No 49487352;
11. Microsoft Office 2007 – лицензия No 44414438;
12. Антивирус Kaspersky – P/N: KL4863RAUFQ;
13. Adobe Acrobat Reader – открытая лицензия.

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы
(обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка
Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/
ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/
Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/
КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/

Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа представляют собой специальные помещения, в состав которых входят специализированная мебель и технические средства обучения.
Специализированная мебель:
парта со скамьей- 52 шт.
учебные места - 104 шт.
рабочее место преподавателя (стол и стул) – 1 шт.
доска аудиторная-1 шт.
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)
2. Проектор Epson EMP-X52
3. Экран для проектора
Технические средства обучения:
Ноутбук ACER AspireES1-523-294D, 15.6", AMDE1 7010
1.5ГГц, 4ГБ, 500ГБ, AMDRadeonR2

Учебные аудитории для проведения практических работ представляют собой компьютерные классы или лаборатории, оснащенные лабораторным оборудованием, в зависимости от степени сложности.
Специализированная мебель:
1. компьютерные столы – 15 шт.
2. стулья – 15 шт.
3. рабочее место преподавателя (стол и стул) – 1 шт.
5. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (15 шт.):
1. компьютерный к-кс Intel Core i5 6500 + монитор Acer 21.5"
K222HQLCbid + клавиатура SVEN Standard 301, мышь CBR
CM-102 (10 шт.)
2. Компьютерный комплекс Option в составе: Системный блок, клавиатура, мышь, монитор (2 шт)
3. Ноутбук Acer AS5738G;
4. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
5. Ноутбук 15,6” ASUS P53S/P53SJ, Intel Core i5
структурированная кабельная система:
1. ком-кс "Сетевое оборудование "Cisco" ч.2
2. концентратор

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС ВолГУ.