Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

| Семестр | Трудоемкость, кред. | Общий объем курса, час. | Лекции, час. | Практич. занятия, час. | Лаборат. работы, час. | В форме практической подготовки/ В | СРС, час. | КСР, час. | Форма(ы) контроля, экз./зач./КР/КП |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 4 | 144 | 30 | 30 | 0 | | 84 | 0 | З КР |
| Итого | 4 | 144 | 30 | 30 | 0 | 0 | 84 | 0 | |

# АННОТАЦИЯ

Целью преподавания дисциплины является: изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина реализует требования образовательного стандарта НИЯУ МИФИ по направлению 10.04.01 «Информационная безопасность» и содействует формированию у студентов профессиональных компетенций, необходимых для решения задач, относящихся к определенному виду профессиональной деятельности.

Целью преподавания дисциплины является: изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

Задачами дисциплины являются:

привитие обучаемым основ культуры обеспечения ИБ;

формирование у обучаемых понимания роли процессов управления в обеспечении ИБ организаций, объектов и систем;

ознакомление обучаемых с основными методами управления ИБ организаций, объектов и систем;

обучение различным методам реализации процессов управления ИБ, направленных на эффективное управление ИБ конкретной организации.

Таким образом, дисциплина «Управление информационной безопасностью» является неотъемлемой составной частью профессиональной подготовки студентов по направлению подготовки 10.04.01 «Информационная безопасность». Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать у студента, и в частности, вырабатывать у него такие качества, как:

строгость в суждениях,

творческое мышление,

организованность и работоспособность,

дисциплинированность,

самостоятельность и ответственность.

## 2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Управление информационной безопасностью» относится к числу дисциплин базовой части профессионального цикла. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыки, сформированные в процессе: − изучения программы общеобразовательной школы;

освоения программы подготовки у стеднтов по родственным направлениям высшего профессионального образования;

изучения дисциплин: «Экономика и управление», «Основы обеспечения непрерывности и информационной безопасности бизнеса», «Защищенные информационные системы». Знания,

полученные при изучении дисциплины «Управление информационной безопасностью» являются базовыми для профессиональных дисциплин, входящих в вариативную часть профессионального цикла учебного плана подготовки по направлению 10.04.01 «Информационная безопасность».

## 3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции |
|---|---|
| ОПК-3 [1] – Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности | З-ОПК-3 [1] – Знать: основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью<br>У-ОПК-3 [1] – Уметь: проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации<br>В-ОПК-3 [1] – Владеть: навыками разработки политик безопасности различных уровней и работы с нормативными правовыми актами в области информационной безопасности |
| УК-1 [1] – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий | З-УК-1 [1] – Знать: методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации<br>У-УК-1 [1] – Уметь: применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации<br>В-УК-1 [1] – Владеть: методологией системного и критического анализа проблемных ситуаций; методиками постановки цели, определения способов ее достижения, разработки стратегий действий |
| УК-3 [1] – Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели | З-УК-3 [1] – Знать: методики формирования команд; методы эффективного руководства коллективами; основные теории лидерства и стили руководства<br>У-УК-3 [1] – Уметь: разрабатывать план групповых и организационных коммуникаций при подготовке и выполнении проекта; сформулировать задачи членам команды для достижения поставленной цели; разрабатывать командную стратегию; применять эффективные стили руководства командой для достижения поставленной цели<br>В-УК-3 [1] – Владеть: умением анализировать, проектировать и организовывать межличностные, |

| | |
|---|---|
| | групповые и организационные коммуникации в команде для достижения поставленной цели; методами организации и управления коллективом |

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

| **Задача профессиональной деятельности (ЗПД)** | **Объект или область знания** | **Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)** | **Код и наименование индикатора достижения профессиональной компетенции** |
|---|---|---|---|
| проектный | | | |
| Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации | Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры | ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности<br><br>*Основание:* Профессиональный стандарт: 06.030, 06.032, 06.033, 06.034 | З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, |

| | | | |
|---|---|---|---|
| | | | методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз |

| | | | |
|---|---|---|---|
| | | | безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации). |
| Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации | Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры | ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ иди информационно-аналитических систем безопасности<br><br>*Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034 | З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного |

| | | | |
|---|---|---|---|
| | | | доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа. ;<br>У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее. ;<br>В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты |

| | | | |
|---|---|---|---|
| | | | информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее. |
| организационно-управленческий | | | |
| Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры | Контроль защищенности информации на объектах информатизации | ПК-7 [1] - Способен планировать и организовывать предпроектное исследование объектов обеспечения ИБ или объектов информационно-аналитических систем безопасности<br><br>*Основание:* Профессиональный стандарт: 06.031 | З-ПК-7[1] - Знать: основные методы организационного обеспечения информационной безопасности иас; основные виды угроз безопасности операционных систем; защитные механизмы и средства обеспечения безопасности операционных систем. ; У-ПК-7[1] - Уметь: организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; определять методы управления доступом, типы доступа и |

| | | | |
|---|---|---|---|
| | | | правила разграничения доступа; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях. ; В-ПК-7[1] - Владеть: основами формирования комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в иас информации ограниченного доступа. |
| Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры | Контроль защищенности информации на объектах информатизации | ПК-8 [1] - Способен использовать навыки составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области ИБ или в области информационно-аналитических систем безопасности<br><br>*Основание:* Профессиональный стандарт: 06.033, 06.034 | З-ПК-8[1] - Знать: профессиональная и криптографическая терминология в области безопасности информации; эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения. |

| | | | |
|---|---|---|---|
| | | | организационно-распорядительная документация по защите информации на объекте информатизации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); технические каналы утечки акустической речевой информации; методы защиты информации от утечки по техническим каналам; способы защиты акустической речевой информации от утечки по техническим каналам. ; У-ПК-8[1] - Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять перечень информации (сведений)ограниченного доступа, подлежащих защите в организации; определять условия расположения объектов информатизации относительно границ контролируемой зоны; разрабатывать аналитическое обоснование необходимости создания |

| | | | |
|---|---|---|---|
| | | | системы защиты информации в организации; разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации. ; В-ПК-8[1] - Владеть: основами применения средств схемотехнического проектирования и современной измерительной аппаратуры; основами оптимизации работ электронных схем с учетом требований по защите информации; основами организации проведения научных исследований по вопросам технической защиты информации, выполняемых в организации. |

## 4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

| № п.п | Наименование раздела учебной дисциплины | Недели | Лекции/ Практ. (семинары )/ Лабораторные работы, час. | Обязат. текущий контроль (форма*, неделя) | Максимальный балл за раздел** | Аттестация раздела (форма*, неделя) | Индикаторы освоения компетенции |
|---|---|---|---|---|---|---|---|
| | *2 Семестр* | | | | | | |
| 1 | Первый раздел | 1-8 | 16/16/0 | | 25 | КИ-8 | З-ОПК-3, У-ОПК-3, З-ПК-1, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | У-ПК-1, З-ПК-2, У-ПК-2, З-ПК-7, У-ПК-7, З-ПК-8, У-ПК-8, З-УК-1, У-УК-1, З-УК-3, У-УК-3 |
| 2 | Второй раздел | 9-15 | 14/14/0 | | 25 | КИ-15 | З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-7, У-ПК-7, В-ПК-7, З-ПК-8, У- |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | ПК-8, В-ПК-8, З-УК-1, У-УК-1, В-УК-1, З-УК-3, У-УК-3, В-УК-3 |
| | *Итого за 2 Семестр* | | 30/30/0 | | 50 | | |
| | **Контрольные мероприятия за 2 Семестр** | | | | 50 | ЗО, КР | З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-7, У-ПК-7, В-ПК-7, З-ПК-8, У-ПК-8, В-ПК-8, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-1, У-ПК-1, В-ПК-1, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-7, У-ПК-7, В-ПК-7, З-ПК-8, У-ПК-8, В-ПК-8, З-УК-1, У-УК-1, В-УК-1, З-УК-3, У-УК-3, В-УК-3 |

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

| **Обозначение** | **Полное наименование** |
|---|---|
| ЗО | Зачет с оценкой |
| КИ | Контроль по итогам |
| З | Зачет |
| КР | Курсовая работа |

## КАЛЕНДАРНЫЙ ПЛАН

| **Недели** | **Темы занятий / Содержание** | **Лек., час.** | **Пр./сем., час.** | **Лаб., час.** |
|---|---|---|---|---|
| | *2 Семестр* | 30 | 30 | 0 |
| **1-8** | **Первый раздел** | 16 | 16 | 0 |
| 1 | **Место дисциплины в учебном плане. Базовая** | Всего аудиторных часов | | |

| | | | | |
|---|---|---|---|---|
| | **терминология**<br>Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами учебного плана. Содержание дисциплины. Виды контроля знаний. Формы проведения занятий. Основы управления ИБ (дистанционное освоение электронного образовательного курса). Термины и определения понятий «информационная безопасность», «система», «управление», «процесс». | 4 | 4 | 0 |
| | | Онлайн | | |
| | | 0 | 0 | 0 |
| 2 - 3 | **Стандартизация систем и процессов управление ИБ**<br>Характеристики стандартов, относящихся к управлению ИБ, стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ, серия стандартов 27000 «Информационная технология. Методы обеспечения безопасности», отраслевые стандарты в области управления ИБ. | Всего аудиторных часов | | |
| | | 4 | 4 | 0 |
| | | Онлайн | | |
| | | 0 | 0 | 0 |
| 4 - 5 | **Политики ИБ**<br>Понятия политики ИБ (ПолИБ), виды ПолИБ, основные требования и принципы, учитываемые при разработке и внедрении ПолИБ, содержание политики ИБ, жизненный цикл политики ИБ, ответственность за исполнение ПолИБ. | Всего аудиторных часов | | |
| | | 4 | 4 | 0 |
| | | Онлайн | | |
| | | 0 | 0 | 0 |
| 6 - 8 | **Управление и система управления ИБ**<br>Необходимость управления ОИБ организации, деятельность по ОИБ организации как процесс, определение управления ИБ организации, цель и задачи управления ИБ организации, уровни и функциональная структура управления ИБ организации, управление ИБ информационно-телекоммуникационных технологий организации, система управления ИБ организации, процессный подход в рамках управления ИБ, работа с процессами СУИБ организации, стратегии построения и внедрения СУИБ. | Всего аудиторных часов | | |
| | | 4 | 4 | 0 |
| | | Онлайн | | |
| | | 0 | 0 | 0 |
| **9-15** | **Второй раздел** | 14 | 14 | 0 |
| 9 - 10 | **Документы в области ИБ**<br>Основные требования к документам. Классификация документов. Документы, относящиеся к первому уровню. Документы, относящиеся ко второму уровню. Документы, относящиеся к третьему уровню. Документы, относящиеся к четвертому уровню. | Всего аудиторных часов | | |
| | | 4 | 4 | 0 |
| | | Онлайн | | |
| | | 0 | 0 | 0 |
| 11 - 15 | **Системы и процессы управления ИБ**<br>Политики ИБ. Процессы управления ИБ. Процессный подход в рамках управления ИБ. Управление ролями ИБ. | Всего аудиторных часов | | |
| | | 10 | 10 | 0 |
| | | Онлайн | | |
| | | 0 | 0 | 0 |

Сокращенные наименования онлайн опций:

| **Обозначение** | **Полное наименование** |
|---|---|
| ЭК | Электронный курс |
| ПМ | Полнотекстовый материал |
| ПЛ | Полнотекстовые лекции |
| ВМ | Видео-материалы |
| АМ | Аудио-материалы |

| | |
|---|---|
| Прз | Презентации |
| Т | Тесты |
| ЭСМ | Электронные справочные материалы |
| ИС | Интерактивный сайт |

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

| **Недели** | **Темы занятий / Содержание** |
|---|---|
| | *2 Семестр* |
| 1 - 2 | **Защита**<br>Защита студентами результатов выполнения первой части первого домашнего ДЗ-1 (презентация) |
| 3 - 4 | **Документы в области ИБ**<br>Документы в области ИБ |
| 5 - 6 | **Защита**<br>Защита студентами результатов выполнения первого домашнего задания ДЗ-1 (презентация) |
| 7 - 8 | **Политики ИБ**<br>Политики ИБ |
| 9 - 10 | **Защита**<br>Защита студентами результатов выполнения первой части второго домашнего задания ДЗ-2 (презентация) |
| 11 - 12 | **Процессный подход в рамках управления ИБ**<br>Процессный подход в рамках управления ИБ |
| 13 - 14 | **Управление ролями ИБ**<br>Управление ролями ИБ |
| 15 - 16 | **Защита**<br>Защита студентами результатов выполнения второго домашнего задания ДЗ-2 (презентация) |

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

С целью формирования и развития профессиональных навыков студентов в дисциплине используются активные и интерактивные формы проведения занятий: доклады и презентации с их обсуждением, ролевые игры с дискуссиями и разбором конкретных ситуаций в сочетании с внеаудиторной работой. В соответствии со спецификой ВУЗа в процессе преподавания дисциплины в каждом разделе выделяются наиболее важные темы и акцентируется на них внимание обучаемых. В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области управления ИБ.

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

| **Компетенция** | **Индикаторы освоения** | **Аттестационное мероприятие (КП 1)** |
|---|---|---|
| ОПК-3 | З-ОПК-3 | ЗО, КР, КИ-8, КИ-15 |
| | У-ОПК-3 | ЗО, КР, КИ-8, КИ-15 |
| | В-ОПК-3 | ЗО, КР, КИ-15 |
| ПК-1 | З-ПК-1 | ЗО, КИ-8, КИ-15 |
| | У-ПК-1 | ЗО, КИ-8, КИ-15 |
| | В-ПК-1 | ЗО, КИ-15 |
| ПК-2 | З-ПК-2 | ЗО, КИ-8, КИ-15 |
| | У-ПК-2 | ЗО, КИ-8, КИ-15 |
| | В-ПК-2 | ЗО, КИ-15 |
| ПК-7 | З-ПК-7 | ЗО, КР, КИ-8, КИ-15 |
| | У-ПК-7 | ЗО, КР, КИ-8, КИ-15 |
| | В-ПК-7 | ЗО, КР, КИ-15 |
| ПК-8 | З-ПК-8 | ЗО, КР, КИ-8, КИ-15 |
| | У-ПК-8 | ЗО, КР, КИ-8, КИ-15 |
| | В-ПК-8 | ЗО, КР, КИ-15 |
| УК-1 | З-УК-1 | ЗО, КИ-8, КИ-15 |
| | У-УК-1 | ЗО, КИ-8, КИ-15 |
| | В-УК-1 | ЗО, КИ-15 |
| УК-3 | З-УК-3 | ЗО, КИ-8, КИ-15 |
| | У-УК-3 | ЗО, КИ-8, КИ-15 |
| | В-УК-3 | ЗО, КИ-15 |

**Шкалы оценки образовательных достижений**

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td></td><td>Оценка «удовлетворительно» выставляется студенту, если он имеет</td></tr>
</table>

| | | | |
|---|---|---|---|
| 60-64 | | E | знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала. |
| Ниже 60 | 2 – «*неудовлетворительно*» | F | Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. |

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

2. ЭИ К65 Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : лабораторный практикум, Москва: НИЯУ МИФИ, 2013

3. ЭИ М60 Сетевые атаки на открытые системы на примере Интранета : учебное пособие для вузов, Москва: НИЯУ МИФИ, 2012

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 О-75 Основы управления информационной безопасностью Кн.1, Москва: Горячая линия - Телеком, 2018

2. 004 М 60 Управление инцидентами информационной безопасности и непрерывностью бизнеса Кн.3 , Москва: Горячая линия - Телеком, 2017

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

## 8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

## 9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной Дисциплины в соответствии с планом лекций, практических занятий и контроля знаний.

Успешное освоение Дисциплины требует от студентов посещения лекций, активной работы во время практических занятий, выполнения всех учебных заданий преподавателя, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение Дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Теория ИБ как наука использует свою терминологию, категориальный, графический и математический аппараты, которыми студент должен научиться пользоваться и применять по ходу записи лекции. Культура записи лекции – один из важнейших факторов успешного и творческого овладения знаниями.

В конце лекции преподаватель оставляет время (5 минут) для того, чтобы студенты имели возможность задать уточняющие вопросы по изучаемому материалу.

Лекции имеют в основном обзорный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов, а также призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной Дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам. С этой целью каждый студент после изучения определенной темы должен проверить уровень своих знаний с помощью вопросов, которые помещены в электронном учебном пособии.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

Помимо этого необходимо особое внимание уделить темам: выбор области деятельности системы управления ИБ, роль руководства в системе управления ИБ, процесс анализа рисков ИБ.

Тема выбора области деятельности СУИБ так важна, потому что именно от того насколько правильно выбрана область деятельности СУИБ зависит то, насколько эффективно будет работать она и все процессы управления безопасностью в рамках этой системы. Область деятельности СУИБ - это область применения и границы СУИБ в терминах характеристик бизнеса, организации, ее местонахождения, ресурсов и технологий. Помимо того, что границы области деятельности необходимо четко определить, их еще необходимо обосновать. Выбор области деятельности будущей СУИБ – не такая простая задача как кажется. В рамках большой организации, предоставляющей внешние услуги своим заказчикам, для выбора области деятельности может потребоваться проведение отдельного проекта. В основе этого проекта будет лежать глубокий анализ существующих бизнес-процессов компании, их взаимосвязи, выходных результатов каждого из процессов и заинтересованных сторон в рамках каждого из процессов. Даже в небольшой организации, где, казалось бы, может быть всего несколько ключевых бизнес-процессов, подобный анализ может оказаться очень полезным, т.к. в результате может быть получена неожиданная картина, в которой проявятся неочевидные взаимосвязи между процессами и фокус критичности бизнес-процессов может быть смещен в неожиданную сторону.

Что касается роли руководства на различных этапах жизни системы управления ИБ, то эта тема важна, потому что, для того чтобы разработка СУИБ была наиболее эффективной и для этой работы были предоставлены все необходимые ресурсы необходимо, чтобы проект по разработке СУИБ был инициирован руководством организации. В таком случае можно быть уверенными в том, что для построения системы будут предоставлены все необходимые ресурсы, все управленческие решения будут также приняты своевременно и с учетом стратегических целей бизнеса организации. В ходе дальнейшей жизни системы может также потребоваться принятие управленческих решений в рамках СУИБ. Прямо выраженная, явная и реальная поддержка со стороны руководства требуется при выполнении следующих процессов и действий: разработка политики ИБ, определение целей системы управления ИБ, распределение ролей и обязанностей, информирование организации о важности управления ИБ для бизнеса, предоставление ресурсов для СУИБ, выбор приемлемого уровня риска, а также проведение управленческого анализа. Студенты должны осознавать, что проекты по построению и внедрению системы управления ИБ невозможны без должной приверженности и заинтересованности руководства организации, т.к. никто кроме высшего руководства организации не уполномочен принимать управленческие решения такого уровня, который требуется для разработки процессов управления и их внедрения. Это очень важно, т.к. даже в самом определении СУИБ говорится о том, что система управления ИБ является частью общей системы управления организации, и все решения, принимаемые в рамках СУИБ, должны учитывать цели и задачи бизнеса организации.

## 10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

При чтении лекций необходимо придерживаться данной последовательности тем, т.к. данная последовательность учитывает жизненный цикл СУИБ и циклическую модель PDCA, которая в свою очередь обеспечивает непрерывное улучшение процессов управления ИБ и СУИБ в целом. При чтении лекций необходимо приводить, по возможности, практические

примеры и особенности реализации тех или иных процессов управления ИБ, для формирования у студентов как теоретических, так и практических навыков разработки процессов управления ИБ и систем управления ИБ в целом.

Практическое занятие/семинар имеет целью научить обучаемых применять теоретические знания при решении практических задач. Это групповое занятие студентов под руководством преподавателя, направленное на выработку и закрепление профессиональных умений и навыков.

Во время проведения семинара особое внимание обращается на активизацию самостоятельной работы студентов над поставленными задачами. Рекомендуется практиковать выдачу обучаемым для самостоятельной работы тем докладов или презентаций и постоянно контролировать их выполнение.

По мере возможности следует практиковать проведение семинаров с использованием средств вычислительной техники в специализированных классах – для демонстрации подготовленных студентами презентаций.

Представленные студентами доклады и презентации и их качество оцениваются преподавателем в рамках текущего контроля успеваемости по дисциплине и вносят свой вклад в аттестацию по разделам дисциплины, по которым они представлены.

Возможные темы докладов и презентаций, которые служат основой для контроля самостоятельной текущей работы студента, формируются в рамках выполнения двух домашних заданий

Автор(ы):

Горбатов Виктор Сергеевич, к.т.н., доцент

Рецензент(ы):

Дураковский А.П.