ПРИЛОЖЕНИЕ 3

Аннотации дисциплин

Оглавление

Защищенные информационные системы – Б1.Б.01

Трудоемкость в зачетных единицах:	**4**	**3 семестр**
Часов (всего) по учебному плану:	**144 ч**	**3 семестр**
Лекции	**16 ч**	**3 семестр**
Практические занятия	**48 ч**	**3 семестр**
Самостоятельная работа	**44 ч**	**3 семестр**
Экзамены/зачеты	**36 ч**	**3 семестр**

Цели дисциплины: формирование знаний и умений по технологиям, методам и средствам создания защищенных информационных систем (ИС) с последующим применением на практике изученных методов в профессиональной деятельности.

Основные разделы дисциплины: Основные подходы к обеспечению защищенности (доверенности) информационных (автоматизированных) систем. Концепция компании Microsoft: безопасность, безотказность, деловая добросовестность. «Оранжевая книга» США, анализ критериев защищенности компьютерных систем. «Общие критерии»: анализ подходов к определению требований и измерению уровней доверия к информационным технологиям. Основы нормативного и методического регулирования разработки и обеспечения функционирования защищенных информационных систем РФ различного назначения: государственные и муниципальные информационные системы (ГИС, МИС), информационные системы персональных данных (ИСПДн), автоматизированных системах управления технологическими процессами на значимых объектах критической информационной инфраструктуры (АСУ ТП КВО). Требования стандартов, регламентирующих создание автоматизированных систем в защищенном исполнении. Математическое и функциональное моделирование механизмов защиты информационных систем (технологий) различного назначения**.** Парадигма «Общих критериев» и применение требований стандартов серии 15408 для определения перечня требований (компонент) безопасности информационных технологий и определения уровня (компонент) доверия к ним. Механизмы защиты информации в информационных (автоматизированных) системах различного назначения. Требования к обеспечению защиты информации в информационных (автоматизированных) системах: ИСПДн, АСУ ТП КИИ, ГИС (МИС). Технология выбора механизмов защиты. Применение системного подхода при выборе механизмов защиты информации. Анализ и оценка уровня защищенности информации в информационных (автоматизированных) системах различного назначения. Практика применения «Общих критериев» при оценке уровня доверия к безопасности информационных систем (технологий). Организация мероприятий по аттестации информационных систем по требованиям безопасности информации.

Технологии обеспечения информационной безопасности объектов – Б1.Б.02

Трудоемкость в зачетных единицах:	**6**	**2 семестр**
Часов (всего) по учебному плану:	**216 ч**	**2 семестр**
Лекции	**16 ч**	**2 семестр**
Практические занятия	**16 ч**	**2 семестр**
Самостоятельная работа	**148 ч**	**2 семестр**
Экзамены/зачеты	**36 ч**	**2 семестр**

Цель дисциплины: формирование знаний и умений по применению технологий обеспечения информационной безопасности сложных социотехнических объектов и систем на основе применения отечественных и международных стандартов, руководящих документов и методик по обеспечению информационной безопасности хозяйствующих субъектов.

Основные разделы дисциплины: Требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации и технологиям защиты информации, принципы работы и устройства технических средств защиты информации. Требования, предъявляемые к процессам защите информации в современных АСУ, АСУ ТП и объектов критической информационной инфраструктуры. Принципы выбора средств и технологий защиты при организации системы информационной безопасности. Классификация технологий обеспечения ИБ: обнаружения вторжений, защиты от НСД, антивирусное программное обеспечение, проактивной защиты информации в корпоративных системах, аудита информационной безопасности. Проблемы развития технологий обеспечения безопасности. Технологии разработки документов при создании системы информационной безопасности (политик, концепций, планов, описаний, технических заданий и процедур).

Управление информационной безопасностью – Б1.Б.03

Трудоемкость в зачетных единицах:	**8**	**2, 3 семестры**
Часов (всего) по учебному плану:	**288 ч**	**2, 3 семестры**
Лекции	**16 ч**	**2 семестр**
Практические занятия	**64 ч**	**2, 3 семестры**
Самостоятельная работа	**133,7 ч**	**2, 3 семестры**
Курсовые проекты (работы)	**16 ч**	**3 семестр**
Экзамены/зачеты	**54 ч**	**2, 3 семестры**

Цели дисциплины: формирование теоретических знаний и умений по организации системы менеджмента информационной безопасности в организациях на основе оценки рисков информационной безопасности, реализации и внедрения соответствующих механизмов контроля, распределения ролей и ответственности, обучения персонала, оперативной работы по осуществлению защитных мероприятий и мониторинга функционирования механизмов контроля.

Основные разделы дисциплины: Требования современных отечественных и международных стандартов по системе менеджмента информационной безопасности (СМИБ). Концепция управления информационной безопасностью на основе цикла Дёминга-Шухарта. Критерии управления информационной безопасностью. Разработка плана и концепции СМИБ. Логистика процессов управления информационной безопасностью на основе стандартов. Система документооборота и её формализованное представление. Политика информационной безопасности и технология её разработки. Частные политики информационной безопасности. Процедуры, регламенты и инструкции по информационной безопасности. Методики моделирования угроз и оценки рисков. Разработка плана по обработке рисков. Разработка положения о применимости. Аттестация хозяйствующих субъектов по требованиям СМИБ: этапы и их последовательность, необходимая документация и механизм процедуры сертификации системы управления информационной безопасностью. Практическая работа по управлению информационной безопасностью на модели хозяйствующего субъекта.

Критерии оценки безопасности информационных технологий – Б1.В.01

Трудоемкость в зачетных единицах:	**5**	**1 семестр**
Часов (всего) по учебному плану:	**180 ч**	**1 семестр**
Лекции	**16 ч**	**1 семестр**
Практические занятия	**48 ч**	**1 семестр**
Самостоятельная работа	**98 ч**	**1 семестр**
Экзамены/зачеты	**18 ч**	**1 семестр**

Цель дисциплины: формирование знаний по разработке постановки задач математического моделирования технических объектов и систем управления (ТССУ), выбор технологий моделирования и практическая реализация задач, обработка и анализ полученных результатов; подготовка к проведению исследований в сфере управления информационной безопасностью и разработка математических моделей для реализации научно-исследовательских проектов.

Основные разделы дисциплины: Виды требований безопасности (функциональные и доверия), основные конструкции представления требований безопасности (профиль защиты, задание по безопасности). Основные методические положения по оценке безопасности ИТ. Универсальный систематизированный каталог функциональных требований безопасности. Систематизированный каталог требований доверия к безопасности и оценочные уровни доверия, определяющие меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

Организационно-правовые механизмы обеспечения информационной безопасности – Б1.В.02

Трудоемкость в зачетных единицах:	**4**	**2 семестр**
Часов (всего) по учебному плану:	**144 ч**	**2 семестр**
Лекции	**16 ч**	**2 семестр**
Практические занятия	**32 ч**	**2 семестр**
Самостоятельная работа	**39,7 ч**	**2 семестр**
Курсовые проекты (работы)	**16 ч**	**2 семестр**
Экзамены/зачеты	**36 ч**	**2 семестр**

Цели дисциплины: формирование у обучаемых знаний о закономерностях функционирования и развития государственной системы информационной безопасности, о системе российского права и его отраслей, которые регулируют вопросы информационной безопасности с последующим применением этих знаний в профессиональной сфере и практических навыков по формированию способности человека правовыми средствами решать те или иные профессиональные задачи.

Основные разделы дисциплины**:** Основные термины и определения в сфере правового обеспечения ИБ. Структура нормативно-правовых актов, регулирующих деятельность в сфере ИБ. Структура, задачи и функции органов, регулирующих деятельность объектов и субъектов в сфере ИБ. Методика анализа нормативно-правовых актов и применения их при организации системы ИБ. Методы работы с нормативно-правовыми документами в практической деятельности. Технологии работы с правовыми базами данных в профессиональных ситуациях в сфере информационной безопасности.

Теоретические основы компьютерной безопасности – Б1.В.03

Трудоемкость в зачетных единицах:	**2**	**3 семестр**
Часов (всего) по учебному плану:	**72 ч**	**3 семестр**
Лекции	**16 ч**	**3 семестр**
Практические занятия	**16 ч**	**3 семестр**
Самостоятельная работа	**22 ч**	**3 семестр**
Экзамены/зачеты	**18 ч**	**3 семестр**

Цели дисциплины: формирование у обучаемых знаний формальных моделей обеспечения безопасности компьютерных систем (моделей компьютерной безопасности), методов и технологий их практической реализации при создании систем информационной безопасности.

Основные разделы дисциплины: Основные понятие и составляющие компьютерной безопасности. Классификация методов и механизмов обеспечения компьютерной безопасности. Понятие угроз безопасности, основы их классификации. Понятие политики безопасности в компьютерных системах и ее формализованное выражение в моделях безопасности. Модели и теоремы безопасности на основе дискреционной политики (пятимерное пространство Хартсона, модель на основе матрицы доступа), модели исследования распространения прав доступа в системах с дискреционной политикой (модель Харисона-Руззо-Ульмана, модель типизованной матрицы доступа, модель TAKE-GRANT, расширенная модель TAKE-GRANT). Недостатки моделей дискреционного доступа, сценарий атаки "троянскими программами". Модели и теоремы безопасности на основе мандатной политики (модели Белла-ЛаПадулы, МакЛина, модель Low-WaterMark). Модели безопасности на основе ролевой политики и технологии рабочих групп пользователей. Понятие и разновидности скрытых каналов утечки информации в компьютерных системах, теоретико-вероятностные основы их выявления и нейтрализации (автоматная модель Гогена-Мессигера). Модели и механизмы обеспечения целостности данных в компьютерных системах (дискреционная модель Кларка-Вильсона, мандатная модель Кена Биба, технологии и протоколы выполнения транзакций в клиент-серверных системах. Понятие и технологии восстановления данных на основе архивирования и журнализации процессов изменения данных, понятие систем и технологий репликации данных. Теоретико-множественные и графовые модели комплексной оценки защищенности компьютерных систем.

Информационно-аналитические системы безопасности – Б1.В.04

Трудоемкость в зачетных единицах:	**5**	**1 семестр**
Часов (всего) по учебному плану:	**180 ч**	**1 семестр**
Лекции	**16 ч**	**1 семестр**
Практические занятия	**48 ч**	**1 семестр**
Самостоятельная работа	**80 ч**	**1 семестр**
Экзамены/зачеты	**36 ч**	**1 семестр**

Цели дисциплины: формирование у обучаемых знаний методов и технологий мониторинга, анализа и обеспечения целостности информации в финансовой, экономической и управленческой деятельности путем интеллектуальной фильтрации совершаемых транзакций в информационных системах с целью противодействия легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

Основные разделы дисциплины: Термины и определения в сфере информационно-аналитического обеспечения информационной безопасности. Задачи информационно-аналитического обеспечения безопасности информационных активов в финансовой, экономической и управленческой деятельности. Методы проведение комплексного анализа функционирования финансовых и экономических структур государственного или системообразующего уровня с целью выявления угроз национальной безопасности. Анализ корректности и устойчивости функционирования национальной системы по противодействию легализации доходов, технологии добывания данных и проведения анализа информационных объектов с признаками подготовки или совершения преступления в финансовой и экономической сферах деятельности. Разработка и применение автоматизированных технологий обработки больших информационных потоков финансовой и экономической информации в режиме реального времени. Ознакомление с технологиями интеллектуальной фильтрации данных биллинговых систем. Моделирование работы биллинговых систем материального, финансового и энергетического учета данных с встроенными сценариями мошеннических действий. Антифродсистемы; цели, назначение, структура, технологии работы и обнаружения мошеннических действий.

Методы и средства защиты информации в системах электронного документооборота_Б1.В.0

Трудоемкость в зачетных единицах:	**4**	**3 семестр**
Часов (всего) по учебному плану:	**144 ч**	**3 семестр**
Лекции	**16 ч**	**3 семестр**
Практические занятия	**32 ч**	**3 семестр**
Лабораторные работы	**16 ч**	**3 семестр**
Самостоятельная работа	**44 ч**	**3 семестр**
Экзамены/зачеты	**36 ч**	**3 семестр**

Цели дисциплины: освоение студентами теоретических знаний области организации систем электронного документооборота, а также формирование профессиональных компетенций, необходимых для реализации методов и средств защиты информации в подобных системах.

Основные разделы дисциплины: Понятие системы электронного документооборота и требования к ее организации. Задачи, функции и структура информационной системы электронного документооборота. Основные виды защищаемой информации в системе электронного оборота документооборота. Угрозы безопасности информации в системах электронного документооборота. Основные требования и меры по защите информации. Технологии защиты электронного документооборота на основе криптографических средств. Моделирование проколов обмены информацией с использованием криптографических средств и систем. Механизмы обеспечения достоверности информации в системах электронного документооборота. Технологии контроля данных при трансграничной передачи информации. Методологические основы разработки информационной системы электронного документооборота. Особенности эксплуатации защищенных систем электронного документооборота.

Трудоемкость в зачетных единицах:	**5**	**1 семестр**
Часов (всего) по учебному плану:	**180 ч**	**1 семестр**
Лекции	**16 ч**	**1 семестр**
Практические занятия	**48 ч**	**1 семестр**
Самостоятельная работа	**80 ч**	**1 семестр**
Экзамены/зачеты	**36 ч**	**1 семестр**

Цели дисциплины: изучение основ знаний, определяющих квалификацию магистра по направлению подготовки «Информационная безопасность», освоение теоретических теории систем и системного анализа применительно к решению прикладных задач обеспечения информационной безопасности предприятия (организации), применение системного подхода и методов и инструментов системного анализа в профессиональной деятельности по управлению информационной безопасностью, приобретение навыков правильного оформления результатов системного анализа. а также формирование системного подхода при решении задач управления информационной безопасностью организации.

Основные разделы дисциплины: Сущность системного подхода и его преимущества. Основные понятия и определения. Принципы системного подхода. Классификация систем. Цель и содержание учебной дисциплины, характеристика ее составляющих; взаимосвязь учебной дисциплины с другими дисциплинами. Основы моделирования сложных систем. Понятие модели. Методы моделирования. Алгоритм построения математической модели. Проблема оценивания сложных систем. Основы теории эффективности. Шкалы. Типы шкал для оценки систем. Сущность и задачи системного анализа. Принципы системного анализа. Этапы и последовательность системного анализа. Методы системного анализа. Функциональное моделирование сложных систем в области управления информационной безопасностью Методология функционального моделирования IDEF0 в системном анализе. Общие сведения о методологии IDEF. Рекомендации по стандартизации РФ в области функционального моделирования. Принципы методологии IDEF0. Состав, свойства и правила разработки IDEF0 – моделей: графические диаграммы, текстовая часть, глоссарий. Виды диаграмм: родительские и дочерние диаграммы. Правила построения диаграмм. Программные средства реализации методологии структурного моделирования IDEF0 и их возможности. Общая характеристика программного средством AllFusion Process Modeler и анализ возможности его применения для системного анализа в области информационной безопасности.

Трудоемкость в зачетных единицах:	**4**	**1 семестр**
Часов (всего) по учебному плану:	**144 ч**	**1 семестр**
Лекции	**16 ч**	**1 семестр**
Практические занятия	**16 ч**	**1 семестр**
Самостоятельная работа	**94 ч**	**1 семестр**
Экзамены/зачеты	**18 ч**	**1 семестр**

Цели дисциплины: формирование теоретических знаний и практических умений по управлению информационной безопасностью сложных социально-технических и производственных систем, использующих информационные технологии и информационные активы.

Основные разделы дисциплины: История развития теории и практики управления социальными, техническими и производственными системами. Ознакомление с передовыми концепциями менеджмента, особенностями управления организациями и современные модели управления; иметь представление о стилях управления. Формирование способности выполнять моделирование и анализ процессов управления сложных социально-технических и производственных систем. Методы принятия управленческих решений. Математические методы, используемые для принятия решений.

М

е

н

е

д

Трудоемкость в зачетных единицах:	**4**	**1 семестр**
Часов (всего) по учебному плану:	**144 ч**	**1 семестр**
Лекции	**16 ч**	**1 семестр**
Практические занятия	**16 ч**	**1 семестр**
Самостоятельная работа	**94 ч**	**1 семестр**
Экзамены/зачеты	**18 ч**	**1 семестр**

Цели дисциплины: формирование теоретических знаний и умений по организации системы менеджмента информационной безопасности в организациях на основе оценки рисков информационной безопасности, реализации и внедрения соответствующих механизмов контроля, распределения ролей и ответственности, обучения персонала, оперативной работы по осуществлению защитных мероприятий и мониторинга функционирования механизмов контроля.

Основные разделы дисциплины: Требования современных отечественных и международных стандартов по системе менеджмента информационной безопасности (СМИБ). Концепция управления информационной безопасностью на основе цикла Дёминга-Шухарта. Критерии управления информационной безопасностью. Разработка плана и концепции СМИБ. Логистика процессов управления информационной безопасностью на основе стандартов. Система документооборота СМИБ и её формализованное представление. Политика информационной безопасности и технология её разработки. Частные политики информационной безопасности. Процедуры, регламенты и инструкции по информационной безопасности. Методики моделирования угроз и оценки рисков. Разработка плана по обработке рисков. Различные технологии моделирования рисков. Многофакторные модели управления рисками. Разработка положения о применимости. Аттестация хозяйствующих субъектов по требованиям СМИБ: этапы и их последовательность, необходимая документация и механизм процедуры сертификации системы управления информационной безопасностью. Практическая работа по управлению информационной безопасностью на модели хозяйствующего субъекта.

Трудоемкость в зачетных единицах:	**3**	**2 семестр**
Часов (всего) по учебному плану:	**108 ч**	**2 семестр**
Лекции	**32 ч**	**2 семестр**
Практические занятия	**32 ч**	**2 семестр**
Самостоятельная работа	**26 ч**	**2 семестр**
Экзамены/зачеты	**18 ч**	**2 семестр**

Цель дисциплины: освоение профессиональных компетенций по моделированию угроз, оценке и анализу рисков информационной безопасности с использованием различных современных методик управления рисками информационной безопасности.

Основные разделы дисциплины: Моделирование угроз информационной безопасности**.** Цели и задачи моделирования угроз информационной безопасности. Различные подходы к формализованному описанию угроз информационной безопасности. Базовая модель угроз: достоинства и недостатки. Современные подходы к моделированию угроз на основе вербального (описательного), параметрического и когнитивного моделирования. Достоинства и недостатки этих подходов к моделированию угроз. . Управление рисками в концепции стандарта NIST. Концепция управления рисками в стандарте США NIST 800-30 «Руководство по управлению информационными рисками ИТ-систем». Управление рисками в концепции стандарта BS 7799-3. Концепция управления рисками в британском стандарте BS-7799-3. Другие концепции управления рисками: COBIT, CORBA и др. Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Область действия стандарта и его применимость. Основные этапы процесса менеджмента риска информационной безопасности: установление контекста, оценка риска, обработка риска, принятие риска, коммуникация риска, мониторинг и переоценка риска информационной безопасности. Многофакторные модели рисков. Понятие «стратегия управления» рисками. Методика анализа рисков с использованием многофакторных моделей. Имитационное моделирование на основе многофакторных моделей. Оценка погрешностей моделирования. Моделирование рисков информационной безопасности на примере модели филиала АКБ. Постановка деловой игры. Анализ исходных данных и результатов аудита информационной безопасности. Анализ бизнес-процессов модели хозяйствующего субъекта. Классификация и оценка ценности информационных активов организации. Моделирование угроз информационной безопасности. Оценка и моделирование рисков при различных стратегиях управления ими. Разработка плана управления рисками. Обоснование предлагаемых решений управления рисками.

Методы планирования управления – Б1.В.ДВ.02.02

Трудоемкость в зачетных единицах:	**3**	**2 семестр**
Часов (всего) по учебному плану:	**108 ч**	**2 семестр**
Лекции	**32 ч**	**2 семестр**
Практические занятия	**32 ч**	**2 семестр**
Самостоятельная работа	**26 ч**	**2 семестр**
Экзамены/зачеты	**18 ч**	**2 семестр**

Цели дисциплины: формирование у обучаемых знаний принципов, методов и технологий планирования управлением процессами создания систем информационной безопасности с учетом возможных временных, ресурсных и случайных рисков нарушений заданных параметров выполнения отдельных процессов (работ и событий).

Основные разделы дисциплины: Сущность и необходимость планирования как создание технологического процесса разработки комплекса мероприятий, определяющих последовательность достижения конкретных целей с учетом возможностей эффективного использования ресурсов. План как результат планирования, включающий достигаемые технические, материальные, технологические и экономические и показатели проекта. Методы разработки планов и научного обоснования его показателей. Сетевой метод планирования и управления. Практическая работа по моделированию последовательности работ и событий на основе сетевого метода планирования и управления. Гантовский метод планирования и управления. Методы оптимизации планов по ресурсам, времени и исполнителям. Планирование ресурсов и способов их использования для достижения целей управления, обоснование мер по расширению ресурсной базы, структуры закупки (приобретения) необходимых ресурсов и сроков их поступления. Выполнение прогнозных расчетов. Моделирование рисков и оценка их последствий. Управление рисками планирования работ. Оценка эффективности планов. Особенности планирования при создании систем информационной безопасности и управлении ими.

Теоретические основы защиты информации от несанкционированного доступа – Б1.В.ДВ.03.01

Трудоемкость в зачетных единицах:	**3**	**2 семестр**
Часов (всего) по учебному плану:	**108 ч**	**2 семестр**
Лекции	**16 ч**	**2 семестр**
Практические занятия	**16 ч**	**2 семестр**
Самостоятельная работа	**40 ч**	**2 семестр**
Экзамены/зачеты	**36 ч**	**2 семестр**

Цели дисциплины: формирование у обучаемых знаний о современных задачах, методах и средствах защиты информации в компьютерных системах, принципах построения систем защиты от угрозы нарушения конфиденциальности, целостности и доступности информации, основные виды политик безопасности, технологии аутентификации, защиты межсетевого взаимодействия, обнаружения вторжений и защиты от вирусов.

Основные разделы дисциплины: Основные понятие и составляющие компьютерной безопасности. Классификация методов и механизмов обеспечения компьютерной безопасности. Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»). Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности информационных технологий Национального института стандартов и технологий и Агентства национальной безопасности США. Канадские критерии безопасности компьютерных систем. Общие критерии оценки безопасности информационных технологий и ГОСТ Р ИСО\МЭК 15408-2002. Международный стандарт информационной безопасности ISO 27002 и ГОСТ Р ИСО\МЭК 27002-2013. Руководящие документы Гостехкомиссии России (ныне Федеральной службы по техническому и экспортному контролю). Анализ стандартов информационной безопасности. Рекомендации X.800 для распределенных систем. Модели и теоремы безопасности на основе дискреционной политики (пятимерное пространство Хартсона, модель на основе матрицы доступа), модели исследования распространения прав доступа в системах с дискреционной политикой (модель Харисона-Руззо-Ульмана, модель типизованной матрицы доступа, модель TAKE-GRANT, расширенная модель TAKE-GRANT). Модели и механизмы обеспечения целостности данных в компьютерных системах (дискреционная модель Кларка-Вильсона, мандатная модель Кена Биба, технологии и протоколы выполнения транзакций в клиент-серверных системах. Теоретико-множественные и графовые модели комплексной оценки защищенности компьютерных систем.

Методы и средства контроля эффективности защиты информации от несанкционированного доступа – Б1.В.ДВ.03.02

Трудоемкость в зачетных единицах:	**3**	**2 семестр**
Часов (всего) по учебному плану:	**108 ч**	**2 семестр**
Лекции	**16 ч**	**2 семестр**
Практические занятия	**16 ч**	**2 семестр**
Самостоятельная работа	**40 ч**	**2 семестр**
Экзамены/зачеты	**36 ч**	**2 семестр**

Цели дисциплины: формирование у обучаемых знаний о современных задачах, методах и средствах защиты информации от несанкционированного доступа, принципах построения систем защиты от угрозы нарушения конфиденциальности, целостности и доступности информации, основные виды политик безопасности, технологии аутентификации, защиты межсетевого взаимодействия, обнаружения вторжений и защиты от вирусов.

Основные разделы дисциплины: Классификация методов и механизмов обеспечения компьютерной безопасности. Понятие угроз безопасности, основы их классификации. Понятие политики безопасности в компьютерных системах и ее формализованное выражение в моделях безопасности. Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»). Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности информационных технологий Национального института стандартов и технологий и Агентства национальной безопасности США. Модели и теоремы безопасности на основе дискреционной политики (пятимерное пространство Хартсона, модель на основе матрицы доступа), модели исследования распространения прав доступа в системах с дискреционной политикой (модель Харисона-Руззо-Ульмана, модель типизованной матрицы доступа, модель TAKE-GRANT, расширенная модель TAKE-GRANT). Недостатки моделей дискреционного доступа, сценарий атаки "троянскими программами". Модели и теоремы безопасности на основе мандатной политики (модели Белла-ЛаПадулы, МакЛина, модель Low-WaterMark). Модели безопасности на основе ролевой политики и технологии рабочих групп пользователей. Понятие и разновидности скрытых каналов утечки информации в компьютерных системах, теоретико-вероятностные основы их выявления и нейтрализации (автоматная модель Гогена-Мессигера). Модели и механизмы обеспечения целостности данных в компьютерных системах (дискреционная модель Кларка-Вильсона, мандатная модель Кена Биба, технологии и протоколы выполнения транзакций в клиент-серверных системах.

Методология инновационных проектов в сфере информационной безопасности – Б1.В.ДВ.04.01

Трудоемкость в зачетных единицах:	**4**	**1 семестр**
Часов (всего) по учебному плану:	**144 ч**	**1 семестр**
Лекции	**16 ч**	**1 семестр**
Практические занятия	**16 ч**	**1 семестр**
Самостоятельная работа	**76 ч**	**1 семестр**
Экзамены/зачеты	**36 ч**	**1 семестр**

Цели дисциплины: формирование знаний и практических по овладению методикой разработки инновационных проектов сфере управления информационной безопасностью на всех стадиях их жизненного цикла от создания инновационной идеи до оценки рисков проекта, расчета показателей его экономической эффективности и планирования практической реализации проекта.

Основные разделы дисциплины: Понятие «инновационный проект», его отличительные особенности, критерии и показатели эффективности инновационных проектов. Классификации инновационных проектов. Сбор, обработка, анализ и систематизация научно-технической информации по теме исследования. Методы, технологии и способы создания инновационных проектов в сфере информационной безопасности. Экономическая эффективность инновационных проектов. Алгоритм реализации инновационного проекта, отражающий все этапы реализации жизненного цикла проекта от разработки бизнес-идеи до оценки экономической эффективности и реализации проекта.

Интеллектуальный анализ данных и процессов – Б1.В.ДВ.04.02

Трудоемкость в зачетных единицах:	**4**	**1 семестр**
Часов (всего) по учебному плану:	**144 ч**	**1 семестр**
Лекции	**16 ч**	**1 семестр**
Практические занятия	**16 ч**	**1 семестр**
Самостоятельная работа	**76 ч**	**1 семестр**
Экзамены/зачеты	**36 ч**	**1 семестр**

Цели дисциплины: формирование у обучаемых знаний принципов, методов, технологий и средств применения систем извлечения знаний методами Data Mining и интеллектуального анализа данных для комплексной оценки безопасности автоматизированных систем управления и разработки систем проактивной защиты информации на основе анализа событий в информационной системе.

Основные разделы дисциплины: Классификация задач, решение которых целесообразно с использованием технологий интеллектуального анализа данных и методов искусственного интеллекта. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений. Классификации технологий интеллектуального анализа данных. Статистические методы обработки данных большого объема (BigDate): корреляционный, кластерный и регрессионный анализ. Выявление латентных переменных методами факторного анализа. Анализ журналов событий. Разработка систем проактивной информационной безопасности на основе анализа событий в информационной системе. Технологии разработки экспертных систем для комплексной оценки безопасности ИС. Практическое использование технологии Data Mining и оболочек экспертных систем. Методы и технологии применения ИТ экспертных систем в профессиональной деятельности.

Аттестация объектов информатизации по требованиям безопасности информации – Б1.В.ДВ.05.01

Трудоемкость в зачетных единицах:	**3**	**3 семестр**
Часов (всего) по учебному плану:	**108 ч**	**3 семестр**
Лекции	**16 ч**	**3 семестр**
Практические занятия	**32 ч**	**3 семестр**
Лабораторные работы	**16 ч**	**3 семестр**
Самостоятельная работа	**26 ч**	**3 семестр**
Экзамены/зачеты	**18 ч**	**3 семестр**

Цели дисциплины: формирование у обучаемых знаний методов и технологий аттестации объектов информатизации требованиям нормативных документов ФСТЭК.

Основные разделы дисциплины: Понятие «аттестация объектов информатизации» как комплекс организационно-технических мероприятий, в результате которых посредством специального документа (Аттестата соответствия) подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации, включающая: анализ исходных данных по аттестуемому объекту информатизации; предварительное ознакомление с аттестуемым объектом информатизации; проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации; проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств; проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации; проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации; анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

***Управление исследованиями и разработками систем защиты информации* – Б1.В.ДВ.05.02**

Трудоемкость в зачетных единицах:	**3**	**3 семестр**
Часов (всего) по учебному плану:	**108 ч**	**3 семестр**
Лекции	**16 ч**	**3 семестр**
Практические занятия	**32 ч**	**3 семестр**
Лабораторные работы	**16 ч**	**3 семестр**
Самостоятельная работа	**26 ч**	**3 семестр**
Экзамены/зачеты	**18 ч**	**3 семестр**

Цели дисциплины: формирование у обучаемых знаний принципов, методов, технологий управления исследованиями и разработками систем защиты информации.

Основные разделы дисциплины: Требования стандарта ГОСТ 15.101-98 «Порядок выполнения НИР» НИР - комплекс исследований, проводимых по единому техническому заданию. Постановка задачи исследования. Анализ существующих взглядов на объект исследований и оценка необходимости его совершенствования. Определение критериев оценки эффективности исследований и их допустимых значений для объекта исследований. Создание научного задела по исследуемой проблеме, исследование вопросов стандартизации и экономики, определение путей создания новых технологических процессов и средств технологического оснащения. Разработка инновационной идеи и оценка реальности её выполнения и эффективности. Разработка технического задания на ОКР по ГОСТ Р 15.201-2000 «Порядок разработки и постановки продукции на производство». Планирование организации исследования, контроля и материального обеспечения. Проведение комплекса работ по исходному ТЗ, с целью разработки (модернизации) продукции. Выполнение комплекса работ с целью обеспечения готовности производства предприятия - изготовителя к изготовлению и поставке вновь разработанных, модернизированных и/или переданных изделий с одного предприятия на другое в заданных объёмах производства.