Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Институт общественных наук
(наименование института (факультета))
Прикладных информационных технологий
(наименование кафедры)

Утверждена

решением кафедры Прикладных информационных технологий ИОН РАНХиГС

Протокол № 9

от «18» мая 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД.6 Защита информации в организационных структурах
(индекс и наименование дисциплины (модуля), в соответствии с учебным планом)

краткое наименование дисциплины (модуля) (при наличии)

38.04.02 Менеджмент
(код и наименование направления подготовки (специальности))

"Digital design в менеджменте (информационно-аналитический менеджмент)"
направленность (профиль/специализация)

Магистр
квалификация

очная
форма(ы) обучения

Год набора - 2018

Москва, 2017 г.

Автор–составитель:
Канд. эконом. наук, доцент кафедры
прикладных информационных технологий Федосеев А.И.
(ученое звание, ученая степень, должность) *(наименование кафедры)*
(Ф.И.О.)

Заведующий кафедрой прикладных ИТ к.т.н. _ Голосов П.Е.
(наименование кафедры) *(ученая степень и(или) ученое звание)* *(Ф.И.О.)*

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы…….....
2. Объем и место дисциплины (модуля) в структуре образовательной программы……...
3. Содержание и структура дисциплины (модуля)……....
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю)……..……...
5. Методические указания для обучающихся по освоению дисциплины (модуля)……...
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю)…….
   6.1. Основная литература……..……...……
   6.2. Дополнительная литература……...……..……
   6.3. Учебно-методическое обеспечение самостоятельной работы…….
   6.4. Нормативные правовые документы…….……..……..
   6.5. Интернет-ресурсы…….……..……...
   6.6. Иные источники…….…….…….……..
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы ……...…..……..

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ОД.6 «Защита информации в организационных структурах» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-1	Способностью управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями	ПК-1.1	Формирование знаний в областях применения и использования методов управления организациями, подразделениями, группами (командами) сотрудников, проектами и сетями
ПК-2	Способностью разрабатывать корпоративную стратегию, программы организационного развития и изменений и обеспечивать их реализацию	ПК-2.1	Формирование знаний для разработки корпоративной стратегии, программы организационного развития и изменений, а также обеспечивать их реализацию

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ *(при наличии профстандарта)*/ профессиональные действия	Код этапа освоения компетенции	Планируемые результаты обучения при прохождении практик*
		на уровне знаний: - Основы делового общения, принципы и методы организации деловых коммуникаций. - Законодательство Российской Федерации, национальных и международных стандартов, руководств и лучших практик по управлению рисками, управлению непрерывностью бизнеса и в чрезвычайных ситуациях. - Основы управления проектами. - Корпоративные нормативные акты организации по политике взаимодействия со средствами массовой информации и связями с общественностью.

ОТФ/ТФ *(при наличии профстандарта)*/ профессиональные действия	Код этапа освоения компетенции	Планируемые результаты обучения при прохождении практик*
		на уровне умений: - Развивать у работников навыки и компетенции, связанные с текущей и будущей работой, используя возможности тренингов. - Проводить интервью и переговоры. - Составлять и проводить презентации и обучающие семинары. - Ставить задачи и контролировать их исполнение. - Отстаивать интересы организации на переговорах по вопросам управления рисками. - Обосновывать позиции по спорным вопросам управления рисками. - Формулировать рекомендации по решению спорных и нестандартных вопросов управления рисками. - Подготавливать план мероприятий по реализации разработанных рекомендаций.
		на уровне навыков: - Подготовка планов и программ консультационных проектов, включающих цели, объем проектов, их сроки и распределение ресурсов для достижения целей консультационных проектов по управлению рисками. - Консультирование руководства организации и работников по вопросам построения и функционирования системы управления рисками. - Идентификация и оценка рисков объекта консультационного проекта (бизнес-процесса, проекта, программы, подразделения). - Оценка схемы построения (эффективность) системы управления рисками или объекта консультационного проекта. - Предложение способов снижения рисков для повышения эффективности объекта консультационного проекта. - Проведение обучающих семинаров для работников организации по вопросам управления рисками.

E Стратегическое корпоративное управление рисками / E/01.8 Определение стратегии организации в части развития и поддержании системы управления рисками	ПК-2.1	на уровне знаний: - Основы теории стратегического менеджмента и маркетинга. - Основные элементы стратегического управления и планирования. - Содержание и взаимосвязь основных элементов процесса стратегического управления. - Основы теории организационных систем. - Основы теории управления изменениями. - Основы финансового менеджмента и бюджетирования. - Принципы формирования бизнес-стратегий. - Принципы разработки стратегии развития системы управления рисками. - Принципы построения и совершенствования систем управления рисками. - Основные тенденции развития международной и российской теории и практики управления рисками. - Структура бюджета организации и системы управления рисками. - Характеристики бизнеса организации. - Корпоративные нормативные акты, определяющие общую стратегию развития организации. - Ключевые бизнес-процессы организации.
		на уровне умений: - Устанавливать и поддерживать деловые контакты, связи, отношения, коммуникации с сотрудниками организации и заинтересованными сторонами по вопросам управления рисками. - Понимать особенности бизнеса организации и его функционирование. - Анализировать общую стратегию организации, стратегии по отдельным видам бизнеса, проектам, бизнес-процессам. - Определять наиболее важные для функционирования организации направления, бизнес-процессы. - Определять приоритетные направления, подверженные наибольшим рискам. - Анализировать внешний и внутренний контекст и проблемные области деятельности организации и потенциальные возможности для развития. - Определять стратегические цели организации с учетом рисков.

		- Разрабатывать стратегию развития системы управления рисками организации на основе современных методов и передовых достижений. - Вносить предложения по изменению и совершенствованию стратегии управления рисками в организации. - Формировать и анализировать показатели эффективности управления рисками в организациию.
		на уровне навыков: - Организация разработки и экспертизы стратегий и политик организации по управлению рисками. - Отбор проектов, выносимых на обсуждение коллегиального органа управления рисками и коллегиального органа управления организацией. - Согласование бюджетов и страховых программ по управлению рисками. - Согласование корпоративных нормативных актов по управлению рисками.

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 2 зачётных единицы (72 часа)

Место дисциплины в структуре ОП ВО

Дисциплина относится к дисциплинам вариативной части профессионального блока Б1.В.ОД.6.

Глубокое усвоение материала обеспечивается сочетанием аудиторных занятий и самостоятельной работы студентов с литературой, языками программирования и нормативными документами. Основным видом учебных занятий по данной дисциплине являются лекционные занятия и лабораторные работы. Лекционные занятия проводятся в виде дискуссий, семинаров, группового проектного обучения, лабораторные – практика по созданию безопасных проектов ПО. Изучение дисциплины осуществляется в течение одного семестра: для студентов очной формы обучения – во 2 семестре. По дисциплине осуществляется текущий контроль самостоятельной работы на дневном обучении и итоговый контроль в форме зачета.

Предшествующими дисциплинами, на которых непосредственно базируется дисциплина «Защита информации в организационных структурах», являются: «Научно-исследовательский семинар "Информационные технологии: Обучение, исследования и разработки"» (Б1.Б.6 - 1 семестр), «Основы разработки интернет-ресурсов» (Б1.В.ОД.2 - 1 семестр), «Программирование» (Б1.В.ДВ2 - 2 семестр). Дисциплина «Защита информации в организационных структурах» является опорой в изучении следующих дисциплин: Б1.В.ДВ.3.2 Управление информационно-технологическими сервисами и контентом (3 семестр), Б2.П.4 Преддипломная практика (4 семестр), Б3 ГИА (4 семестр).

3. Содержание и структура дисциплины

Содержание дисциплины должно соотноситься с планируемыми результатами обучения по дисциплине через задачи, формируемые компетенции и их компоненты (знания, умения, навыки) (Табл. 1).

Таблица 1.

Очная форма обучения

Структура дисциплины (модуля)

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий					
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
Тема 1	Введение. Безопасность функционирования современной организации и технологий.	8	2				6	Т, К
Тема 2	Современная доктрина информационной безопасности Российской Федерации.	10	2				8	Т, К
Тема 3	Международные стандарты информационного обмена. Модели безопасности и их применение.	12		4			8	Т, К
Тема 4	Сущность и задачи обеспечения информационной безопасности.	14	2	4			8	Т, К
Тема 5	Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.	14		6			8	Т, К
Тема 6	Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.	14	2	4			8	Т, К
Промежуточная аттестация								зачет
	Всего:	72	8	18			46	

Примечание: 4 – формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э), реферат (Р), диспут (Д) и др.

Содержание дисциплины

Тема 1. Введение. Безопасность функционирования современной организации и технологий.

Введение. Предмет и задачи дисциплины. Значение и место дисциплины в подготовке специалистов в области прикладных аспектов информатики и информационных технологий по защите информации от несанкционированных воздействий и обеспечения достоверности и целостности при ее обработке в информационно-телекоммуникационных системах. Научная и учебная взаимосвязь дисциплины с другими дисциплинами, изучаемыми в высшем учебном заведении.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения практических и семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Форма проверки знаний. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения дисциплины.

Актуальность проблемы обеспечения информационной безопасности в торгово-экономических структурах, потенциально возможные несанкционированные воздействия на информационную инфраструктуру торгово-экономической деятельности, информационный криминал. Статистические показатели состояния информационной безопасности информационной инфраструктуры торгово-экономической деятельности, динамика ее развития.

Составляющие воздействий на информационную инфраструктуру государства: информационная война, информационный терроризм, информационный криминал. Понятие конкурентной разведки.

Тема 2. Современная доктрина информационной безопасности Российской Федерации.

Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Значение информационной безопасности и ее место в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации.

Международные стандарты информационного обмена, правовые основы защиты государственной, коммерческой, служебной, процессуальной, профессиональной тайны и информации персонального характера. Федеральные Законы Российской Федерации по обеспечению информационной безопасности в информационных технологиях, Доктрина Информационной безопасности Российской Федерации, Концепция Национальной Безопасности Российской Федерации, нормативные и руководящие документы, Постановления Правительства Российской Федерации по проблемам обеспечения информационной безопасности, Руководящие документы и инструкции Федеральной службы по техническому и экспортному контролю (ФСТЭК), Приказы и распоряжения ФСБ РФ, Ведомственные приказы и распоряжения.

Тема 3. Международные стандарты информационного обмена. Модели безопасности и их применение.

Безопасность в сетях Internet и Intranet. Технология безопасности: межсетевые экраны (Межсетевые экраны прикладного уровня, межсетевые экраны с пакетной фильтрацией, гибридные межсетевые экраны). Разработка конфигурации межсетевого экрана: Архитектура 1 – системы за пределами; архитектура 2 – один межсетевой экран; архитектура 3 – двойные межсетевые экраны. Безопасность виртуальных частных сетей (VPN).

Модели безопасности: модели разграничения доступа; модели разграничения доступа, построенные по принципу предоставления прав; модели дискретного доступа; модели мандатного доступа; модель Белла и Лападула; специализированные модели; вероятностные модели; информационные модели; модели контроля целостности; Модель Биба; модель Кларка-Вилсона. Модели анализа безопасности программного обеспечения.

Тема 4. Сущность и задачи обеспечения информационной безопасности.

Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Агрегация информационных ресурсов с точки зрения информационной безопасности. Классификация угроз информационной безопасности. Информационная безопасность компьютерных систем. Основные понятия и определения. Безопасность автоматизированных систем обработки информации. Доступ к информации (санкционированный, несанкционированный), разграничение доступа, конфиденциальность данных, угрозы безопасности, защита информации, политика безопасности

Основные виды угроз безопасности компьютерным системам: нарушения конфиденциальности информации, нарушения целостности информации, нарушения работоспособности системы. Каналы несанкционированного доступа. Способы несанкционированного доступа: перехват паролей, «маскарад», незаконное использование привилегий.

Тема 5. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

«Врожденные слабости» наиболее распространенных служб Internet. Основные компоненты межсетевых экранов: фильтрующие маршрутизаторы, шлюзы сетевого уровня, шлюзы прикладного уровня. Аутентификация пользователей как основной компонент межсетевых экранов. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей. Программные методы защиты сетевых технологий в Internet структурах.

Тема 6. Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.

Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования, Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования. Привязка к внешним (добавляемым) элементам ПЭВМ.

Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Защита информации в организационных структурах используются следующие методы текущего контроля и успеваемости обучающихся:

– при проведении занятий лекционного типа:
опрос (О), эссе (Э), реферат (Р), диспут (Д).

– при проведении занятий семинарского типа:
опрос (О), коллоквиум (К), эссе (Э), реферат (Р), диспут (Д).

– при проведении лабораторных и практических занятий:
опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э), реферат (Р), диспут (Д).

4.1.2. Промежуточная аттестация проводится в форме:
зачета.

4.2. Материалы текущего контроля успеваемости.

Ввариванты тестовых заданий

1. **Проекты, формы** и **модули интернет-приложений** сохраняются с расширениями:

- □ *.vba, *.fex, *.mex;
- □ *.vbp, *.frm, *.bas;
- □ *.exe, *.com, *.bat;
- □ *.htm, *.html

2. **Макросы** и **процедуры** проекта в приложениях сохраняются в разделе проводника:

- □ Macros;
- □ Project;
- □ Module;

3. Свойство **ControlSourse** элемента управления хранит в себе:

- □ Значение присоединенных к элементу данных;
- □ Диапазон присоединенных к элементу данных;
- □ Количество присоединенных к элементу данных;

4. Свойство **BoundValue** хранит в себе:

- □ Количество элементов, находящихся в данный момент в фокусе;
- □ Значение элемента, находящегося в данный момент в фокусе;
- □ Количество связанных между собой элементов;

5. Оператор **Range** задает:

- □ Допустимый в процедуре формат данных;
- □ Допустимый диапазон значений данных;
- □ Обращение к конкретной ячейке или диапазону ячеек;

6. Для того чтобы создать **присоединенный элемент управления** нужно:

- □ Вызвать панель инструментов *Формы* для выбора элемента;
- □ Вызвать панель инструментов *Visual Basic* для выбора элемента;
- □ Вызвать панель инструментов *Элементы управления* для выбора элемента;

7. Для того чтобы войти в **редактор JavaScript** нужно:

- □ Подать команду *Сервис* \ *Макрос* \ *Редактор Visual Basic*;
- □ Вызвать панель инструментов *Visual Basic*;
- □ Нажать клавиши Alt + F11;

8. Вновь записываемый **макрос** может быть доступен:

- □ Только для шаблона Normal.dot;
- □ Только для текущего документа;
- □ Для шаблона Normal.dot или для текущего документа;

9. **Пользовательскую панель инструментов** в можно создать с помощью:

- □ Команды *Сервис* \ *Настройка*, вкладка *Панели инструментов*;
- □ Команды *Вставка* \ *Объект*, параметр *Пакет*;
- □ Команды *Вид* \ *Панели инструментов* \ *Настройка*;
- □ Команды *Вид* \ *Линейка*;

10. **Кнопку для макроса** можно создать с помощью:

- □ Команды *Сервис* \ *Настройка*, вкладка *Команды*;
- □ Команды *Правка* \ *Специальная вставка*;
- □ Команды *Формат* \ *Тема*;

11. Каждый раз при записи **макроса** в проводник проекта добавляется:

- □ Модуль NewMacrosN() в раздел Normal;
- □ Модуль NewMacrosN() в раздел Project;
- □ Процедура Sub <Имя_Макроса>N()...End Sub в модуль NewMacros;

12. **Библиотека динамической компоновки** это:

- □ Файл с расширением *.sys, хранящий все пользовательские настройки;
- □ Файл с расширением *.ini, инициализирующий все макросы, записанные пользователем;
- □ Файл с расширением *.dll, содержащий функции, доступные для коррекции пользователем;

13. Оператор **Alias** указывает:

- □ наличие ошибки в функции из динамической библиотеки;
- □ название (имя) функции, используемое внутри файла *.dll;
- □ наличие вируса в макросе, использующем функцию из динамической библиотеки;

Варианты контрольных работ

1. Основные виды угроз безопасности компьютерных систем.
2. Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.
3. Структурные составляющие гипотетической модели нарушителя.
4. Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.
5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях.

6. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.
7. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.

Примерные темы для контрольных работ

1. Политика безопасности.
2. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.
3. Этапы построения системы защиты автоматизированных информационных систем.
4. Составляющие отдельных этапов.
5. Основные задачи методов защиты информации в автоматизированных информационных системах.
6. Принципы системы защиты информации в АСОИ.

4.3. Оценочные средства для промежуточной аттестации.
4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-1	Способностью управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями	ПК-1.1	Формирование знаний в областях применения и использования методов управления организациями, подразделениями, группами (командами) сотрудников, проектами и сетями
ПК-2	Способностью разрабатывать корпоративную стратегию, программы организационного развития и изменений и обеспечивать их реализацию	ПК-2.1	Формирование знаний для разработки корпоративной стратегии, программы организационного развития и изменений, а также обеспечивать их реализацию

4.3.2 Типовые оценочные средства

Вопросы к зачету по дисциплине «Защита информации в организационных структурах»

1. Понятие «Информационная безопасность». Основные методологические и нормативно-правовые документы по информационной безопасности.

2. Основные понятия по защите компьютерных данных. Доступ к информации, санкционированный доступ, несанкционированный доступ, конфиденциальность данных,

субъект и объект информационных технологий, доступность компонента или ресурса системы, угроза безопасности автоматизированной информационной системе, ущерб безопасности, уязвимость АСОИ, атака на компьютерную систему, политика безопасности.

3. Основные виды угроз безопасности компьютерных систем, Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.

4. Структурные составляющие гипотетической модели нарушителя, Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.

5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.

6. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.

7. Политика безопасности. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.

8. Этапы построения системы защиты автоматизированных информационных систем. Составляющие отдельных этапов.

9. Основные задачи методов защиты информации в автоматизированных информационных системах. Принципы системы защиты информации в АСОИ.

10. Принципы криптографической защиты информации. Криптология, криптография, стеганография, криптоанализ. Три класса криптографических систем.

11. Традиционные симметричные криптографические системы. Ключ шифрования данных, шифры криптографической защиты данных: шифры перестановок, шифры замены, шифры гаммирования, шифры, основанные на аналитических преобразованиях шифруемых данных.

12. Шифрующие таблицы без ключевого слова.

13. Табличное шифрование методов перестановки по ключевому слову или фразе, задающими перестановку.

14. Табличное шифрование методом двойной перестановки.

15. Шифр Цезаря.

16. Метод аффинной системы подстановок Цезаря.

17. Система шифрования Цезаря с ключевым словом.

18. Одноалфавитные монограммные таблицы Трисимуса.

19. Шифры сложной замены. Шифр Гронсфельда.

20. Система шифрования Вернама.

21. Шифрование методом гаммирования.

22. Современные симметричные криптосистемы.

23. Стандарт шифрования DES.

24. Алгоритм шифрования IDEA.

25. Отечественный стандарт шифрования данных ГОСТ 28147-89.

26. Концепция криптографической системы с открытым ключом. Система асимметричной криптографической системы.

27. Однонаправленные Хэш-функции.

28. Криптографическая система шифрования данных RSA.

29. Процедура шифрования и расширения данных в криптографической системе RSA.

30. Безопасность и быстродействие криптографической системы RSA.

31. Схема шифрования Полига-Хелмана.

32. Схема шифрования Эль Гамаля.

33. Комбинированный метод шифрования данных.

34. Электронная цифровая подпись. Правовые основы электронной цифровой подписи. Федеральный закон РФ «Об электронной подписи.

35. Проблема аутентификации данных и электронная цифровая подпись.

36. Однонаправленные Хэш-функции. Алгоритмы электронной цифровой подписи.

37. Алгоритм ЭЦП RSA.

38. Алгоритм ЭЦП Эль Гамаля.

39. Алгоритм ЭПЦ DSA.

40. Отечественный стандарт электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001.

41. Идентификация и проверка подлинности электронных документов и пользователей компьютерных технологий.

42. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверки подлинности пользователей.

43. Процедура «рукопожатия».

44. Протоколы аутентификации с нулевой передачей знаний.

45. Параллельная идентификация с нулевой передачей знаний.

46. Система идентификации Гиллоу-Куискуотера.

47. Управление криптографическими ключами. Генерация и хранение ключей.

48. Иерархия ключей шифрования данных в корпоративных компьютерных системах.

49. Распределение ключей в корпоративных компьютерных системах. Использование одного или нескольких центров распределении ключей. Прямой обмен сеансовыми ключами между санкционированными пользователями.

50. Механизм запроса – ответа в сетевых технологиях, механизм отметки времени.

51. Распределение ключей с участием Центра распределении ключей.

52. Протокол для симметричных криптосистем с использованием отметки времени.

53. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.

54. Алгоритм открытого распределения ключей Диффи-Хелмана.

55. Протокол SKIP управления криптоключами.

56. Аутентификация пользователей как основной компонент межсетевых экранов.

57. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей.

58. Программные методы защиты сетевых технологий в Internet структурах.

59. Защита данных в электронных платежных системах.

60. Принципы функционирования электронных платежных систем.

61. Электронные пластиковые карты. Пассивные и активные пластиковые карты. Основные типы активных пластиковых карт: карты-счетчики, карты с памятью, карты с микропроцессором, карты с контактным считыванием, карты с индукционным считванием.

62. Персональный идентификационный номер (PIN). Обеспечение безопасности электронно-платежной системы POS (Point-of-Sale), схема функционирования POS.

63. Обеспечение безопасности банкоматов в электронных платежных системах, схема обмена сообщениями между банкоматом и хост-ЭВМ банка рои идентификации и платеже, схема прохождения данных с PIN клиента между банкоматом, банком-эквайером и банком-эмитентом.

64. Универсальная платежная система UEPS (Universal Electronic Payment System), состав и архитектура платежной системы, распределение ключей и паролей, цикл платежной транзакции.

65. Торговые терминалы, формирование сессионных ключей, эмиссия карточек, разграничение ответственности между банками-участниками общей платежной системы, двойное шифрование записи о транзакции на ключах банка-эквайера и банка-эмитента.

66. Обеспечение безопасности электронных платежей через сеть Internet.

67. Авторизация и шифрование финансовой информации в сети Internet.

68. Протоколы шифрования SSL (Secure Socket Layer) и SET (Secure Electronic Transactions), использование сертификатов.

69. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

70. Средства и системы управления контролем доступа в компьютерных технологиях.

71. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа. Разграничения доступа к файлам.

72. Защита программного продукта от несанкционированного копирования.

73. Несанкционированное копирование программ как тип НСД.

74. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.

75. Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования.

76. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования.

77. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения.

78. Методы «водяных знаков» и методы «отпечатков пальцев».

79. Защита программного продукта от изучения.

80. Изучение и обратное проектирование программного обеспечения: понятие изучения и обратного проектирования программного обеспечения, способы изучения программного обеспечения (статическое и динамическое изучение), временная надежность (невозможность обеспечения гарантированной надежности).

81. Задачи защиты программного продукта от изучения и способы их решений: защита от отладки, динамическое преобразование кода,

82. Итеративный программный замок А. Долгина

83. Принцип ловушек и принцип избыточного кода, защита от дизассемблирования, принцип внешней загрузки файлов, динамическая модификация программы, защита от трассировки по прерываниям.

84. Аспекты защиты от исследования: способы ассоцианирования защиты и программного обеспечения, оценка надежности защиты от отладки.

85. Защита от разрушающих программных воздействий.

86. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия.

87. Понятие изолированной программной среды.

Уровень освоения компетенций по дисциплине «Защита информации в организационных структурах» определяется:

По компетенции ПК-1:

способностью управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями.

Для приобретения следующих знаний:

- модели поведения экономических агентов и рынков;
- основные информационные технологии управления бизнес-процессами;
- понятийный и терминологический аппарат в области управления экономикой;
- системы сбора, обработки и подготовки информации по предприятию и его внутренним подразделениям.

следующих умений:

- управлять развитием организации осуществлять анализ и разработку стратегии организации на основе современных методов и передовых научных достижений;
- формализовано описывать проект как объект управления экономикой;
- осуществлять анализ государственного планирования экономикой.

следующих навыков:

- навыками количественного и качественного анализа для принятия управленческих решений;
- методикой построения организационно-управленческих моделей;
- способами анализа, синтеза, обобщения информации.

По компетенции ПК-2:

способностью разрабатывать корпоративную стратегию, программы организационного развития и изменений и обеспечивать их реализацию.

Для приобретения следующих знаний:

- основные концепции и методы анализа и выбора нововведений;
- взаимосвязи экономической активности и конкурентоспособного развития предприятий туриндустрии;
- модели и методы прогнозирования экономической деятельности туристских комплексов.

следующих умений:

- идентифицировать и анализировать риски экономических проектов развития объектов и формировать подходы к управлению этими рисками;
- оценивать результаты производственной деятельности и выявлять резервы повышения эффективности производства;
- применять инструментальные (программно-технические) средства управления

проектами;
- решать на примере конкретных ситуаций проблемы выгодности новой продукции (работ, услуг), изменения объема и ассортимента продукции (услуг), капитальных вложений.

следующих навыков:
- специальными методами экономического управленческого анализа;
- инструментарием для составления прогноза основных социально-экономических показателей деятельности предприятий.

Низкий «неудовлетворительно/незачет» - компетенция не освоена или освоена в недостаточной мере. Студент не знает, либо знает на слабом уровне теоретический материал по дисциплине. Не владеет терминологией и основными понятиями из профессиональной сферы или называет неуверенно, с ошибками.

Пороговый (базовый) «удовлетворительно/зачет» - компетенция освоена удовлетворительно, но достаточно. Студент освоил основную базу теоретических знаний. Владеет терминологией и основными понятиями из профессиональной сферы.

Продвинутый «хорошо/зачет» - компетенция освоена достаточно хорошо. Студент знает теоретический материал по дисциплине, умеет применить эти знания на практике. Чётко и ясно формулирует свои мысли. Знает специальную и публицистическую литературу по профессиональным вопросам.

Высокий «отлично/зачет» - компетенция освоена в полной мере или на продвинутом уровне. Студент знает теоретический материал, умеет применить эти знания на практике и имеет опыт в профессионально-практической деятельности. Приводит актуальные примеры из сферы профессиональной деятельности; демонстрирует способности к нестандартной интерпретации поставленного вопроса.

Шкала оценивания.

Оценивание обучаемого на Зачете по дисциплине «Защита информации в организационных структурах».

Баллы (рейтинговой оценки), %	**Оценка**	**Требования к знаниям**
100-81	5, «отлично»	– Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает его на Зачете, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение. – Учебные достижения в семестровый период и результатами рубежного контроля демонстрируют высокую степень овладения программным материалом.

80-61	4, «хорошо»	– Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. – Учебные достижения в семестровый период и результатами рубежного контроля демонстрируют хорошую степень овладения программным материалом.
60-41	3, «удовлетво-рительно»	– Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. – Учебные достижения в семестровый период и результатами рубежного контроля демонстрируют достаточную (удовлетворительную) степень овладения программным материалом.
40-0	2, «неудовлет-ворительно»	– Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. – Учебные достижения в семестровый период и результатами рубежного контроля демонстрировали не высокую степень овладения программным материалом по минимальной планке.

4.4. Методические материалы

При реализации дисциплины «Защита информации в организационных структурах» направления Менеджмент бакалавриата используются интерактивные формы проведения занятий.

Поскольку интерактивное обучение – это, прежде всего, диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, в том числе с использованием информационных технологий и технических средств. Для решения воспитательных и учебных задач в дисциплине «Защита информации в организационных структурах» в рамках коллоквиумов используются следующие интерактивные формы:

- круглый стол (дискуссия, дебаты);
- кейс-метод (разбор конкретных производственных ситуаций);
- метод проектов;
- работа в малых группах.

Кроме того, в процессе обучения задействована такая форма диалогового обучения, как компьютерное рубежное тестирование студентов по разделам дисциплины.

В рамках развития интерактивных форм обучения на дисциплине «Защита информации в организационных структурах» разработаны презентации с возможностью использования различных вспомогательных средств: интерактивной доски, книг, видео, слайдов, компьютеров и т.п. Удельный вес занятий, проводимых в интерактивных формах по дисциплине, представлен таблицей ниже.

Интерактивные методы обучения, используемые на семинарских занятиях дисциплины «Защита информации в организационных структурах»

Семестр	**Вид занятия**	**Используемые интерактивные образовательные технологии**	**Кол-во часов**
	ЛР	Презентации, круглый стол, ролевые игры, кейс-метод, метод проектов, работа в малых группах	2
	ЛР	Использование интегрированных сред.	2
	ЛР	Инструментарий разработки программных приложений.	4
	ЛР	Клиентские сценарии и приложения.	4
ИТОГО:			**12**

Общее количество часов, используемых в аудиторных занятиях дисциплины в интерактивной форме, составляет 12 часов или 37% от 36 часов аудиторных.

5. Методические указания для обучающихся по освоению дисциплины
Методические рекомендации по выполнению заданий самостоятельной работы

Темы эссе по дисциплине «Защита информации в организационных структурах»

1. Программные методы защиты сетевых технологий в Internet структурах.
2. Защита данных в электронных системах коммуникаций.
3. Принципы функционирования электронных платежных систем.
4. Электронные пластиковые карты. Пассивные и активные пластиковые карты. Основные типы активных пластиковых карт: карты-счетчики, карты с памятью, карты с микропроцессором, карты с контактным считыванием, карты с индукционным считванием.
5. Персональный идентификационный номер (PIN).
6. Обеспечение безопасности коммуникационной системы POS (Point-of-Sale), схема функционирования POS.
7. Обеспечение безопасности банкоматов в электронных платежных системах, схема обмена сообщениями между банкоматом и хост-ЭВМ банка рои идентификации и

платеже, схема прохождения данных с PIN клиента между банкоматом, банком-эквайером и банком-эмитентом.

Критерии оценки эссе:

Оценка «удовлетворительно» предполагает, что полученные результаты в значительной степени соответствуют поставленной цели (цель работы достигнута в основном). Обоснована актуальность работы. В процессе анализа литературы отобраны наиболее важные источники, продемонстрировано понимание решаемой проблемы. Выбраны адекватные цели научный подход, методы, процедуры. Они в значительной степени реализованы в работе. Выводы имеют наглядный и проверяемый характер. Требования по оформлению работы в основном выполнены.

Оценка «хорошо» ставится, когда полученные результаты преимущественносоответствуют поставленной цели и задачам. Обоснована практическая и теоретическая актуальность работы. В процессе анализа литературы отобран и проанализирован широкий круг теоретических и эмпирических источников. Выбраны и обоснованы применяемые научные подходы, методы и процедуры. Полученные результаты в целом логичны, доказательны и систематизированы. Оформление работы в целом соответствует существующим требованиям.

Оценка «отлично» предполагает: полученные результаты полностью соответствуют поставленной цели. Обоснована практическая и теоретическая значимость работы. Проведен детальный анализ теоретических и эмпирических источников, выводы автора самостоятельны и аргументированы. Выбраны и подробно описаны применяемые в работе научные подходы, методы и процедуры. Содержание работы полностью отражает узловые проблемы темы, исследовательская часть (в курсовой работе) выполнена самостоятельно, методологически корректно и содержит достоверные и интересные выводы и положения. Оформление работы полностью отвечает всем требованиям

Вопросы к диспуту по дисциплине «Защита информации в организационных структурах»

Теоретические:

1. Протоколы шифрования SSL (Secure Socket Layer) и SET (Secure Electronic Transactions), использование сертификатов.
2. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.
3. Средства и системы управления контролем доступа в компьютерных технологиях.
4. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа. Разграничения доступа к файлам.
5. Защита программного продукта от несанкционированного копирования.
6. Несанкционированное копирование программ как тип НСД.
7. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.
8. Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования.
9. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования.
10. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения.

Прикладные:

1. Протокол для симметричных криптосистем с использованием отметки времени.
2. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
3. Алгоритм открытого распределения ключей Диффи-Хелмана.
4. Протокол SKIP управления криптоключами.
5. Аутентификация пользователей как основной компонент межсетевых экранов.
6. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей.

Вопросы к коллоквиуму по дисциплине «Защита информации в организационных структурах»

1. Управление криптографическими ключами. Генерация и хранение ключей.
2. Иерархия ключей шифрования данных в корпоративных компьютерных системах.
3. Распределение ключей в корпоративных компьютерных системах. Использование одного или нескольких центров распределении ключей. Прямой обмен сеансовыми ключами между санкционированными пользователями.
4. Механизм запроса – ответа в сетевых технологиях, механизм отметки времени.
5. Распределение ключей с участием Центра распределении ключей.

Критерии правильности ответов на вопросы для диспута и коллоквиума:

При оценке ответов на вопросы для диспута и коллоквиума учитывается в первую очередь уровень теоретической подготовки студента (владение категориальным аппаратом, знание нормативно-правовых основ предмета), умение применять имеющиеся знания на практике (пояснить то или иное положение на примере), а также умение высказывать свое мнение, отстаивать свою позицию, слушать и оценивать различные точки зрения, конструктивно полемизировать, находить точки соприкосновения разных позиций.

Тестовые задания для промежуточного контроля и аттестации обучаемых

Спецификация тестового материала

№ п п	Структура учебной дисциплины, наименование разделов и тем*	Количество ТЗ	Количество форм ТЗ			Мера трудности		
			С выбором одного правильного ответа	С выбором нескольких правильных ответов	Графическая форма ТЗ	легкие	средние	трудные
1.	Введение. Безопасность функционирования современной организации и технологий.	5	5	2		3	2	
2.	Современная доктрина информацион	5	5		2	3	2	

	ной безопасности Российской Федерации.							
3.	Международные стандарты информационного обмена. Модели безопасности и их применение.	5	5		5	3	2	
4.	Сущность и задачи обеспечения информационной безопасности.	5	5		7	3	2	
5	Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.	5	5	3		3	2	
6	Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.	5	5	2		3	2	

Самостоятельная работа обучаемого, изучающего дисциплину «Защита информации в организационных структурах» направлена на формирование следующих умений и навыков:

- определения требований и состава средств, методов и мероприятий по организации безопасного обмена информацией в информационных технологиях;
- использование методов организации, планирования и контроля функционирования комплекса средств доступа к ИС;
- практического применения технических, программных и программно-аппаратных средств и методов защиты программных приложений;

- организации системы управления контролем доступа в сетевых компьютерных технологиях и оценку эффективности их безопасного функционирования.
- пользования библиотеками прикладных программ компьютерных систем для решения задач по безопасности программных приложений;
- применения стандартов по проблемам защиты информационных технологий в своей профессиональной деятельности;
- использования специальных программных средств при создании программных приложений и реализации ПО.

Вопросы и задания для самостоятельной подготовки

1. Понятие «Информационная безопасность».
2. Основные методологические и нормативно-правовые документы по информационной безопасности.
3. Основные понятия по защите компьютерных данных.
4. Доступ к информации, санкционированный доступ, несанкционированный доступ.
5. Конфиденциальность данных, субъект и объект информационных технологий, доступность компонента или ресурса системы.
6. Угроза безопасности автоматизированной информационной системе.
7. Ущерб безопасности, уязвимость АСОИ, атака на компьютерную систему, политика безопасности.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Запечников С.В., Казарин О.В., Тарасов А.А КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. М: Юрайт, 2016.

2. Васильева И.Н. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. - М: Юрайт, http://www.biblio-online.ru/, 2016.

6.2. Дополнительная литература.

3. Алексеев В.А. Методы и средства криптографической защиты информации – М.: IPRbooks, http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/17710.html, 2012.

4. Полякова Т.А. ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. - М: Юрайт, http://www.biblio-online.ru/, 2016.

6.3. Учебно-методическое обеспечение самостоятельной работы.

5. Д.П. Зегжда и др. Основы безопасности информационных систем. М., 2000.

6. Джилад Б. Конкурентная разведка. Как распознать внешние риски и управлять ситуацией. – СПб.: Питер, 2010. – 320 с.

7. Леле М. Абсолютное оружие. Как убить конкуренцию: захват и удержание рынка. - М.: ИД «Коммерсантъ»; СПб: ИД «Питер», 2009. – 224 с.

6.4. Нормативные правовые документы.

8. Доктрина информационной безопасности Российской Федерации.

9. Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27 июля 2006 года.
10. Федеральный закон от 4 июля 1996 г. «Об участие в международном информационном обмене».
11. Федеральный закон от 06 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
12. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. N1300. (В редакции Указа Президента Российской Федерации от 10 января 2000 г. N24.
13. Федеральный закон от 3 февраля 1996 г. N17-ФЗ «О банках и банковской деятельности».
14. Федеральный закон от 22 апреля 1996 г. N39-ФЗ «О рынке ценных бумаг».
15. Федеральный закон от 21 ноября 1996 г. N129-ФЗ «О бухгалтерском учете».
16. Окинавская хартия глобального информационного общества. Принята 22 июля 2000 года. Окинава.
17. Приказ ФСБ РФ №66 от 9 февраля 2005 года «Об утверждении Положения о разработке, производстве, реализации т эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
18. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» №351 от 17 марта 2002 года.
19. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
20. ФСТК России. Руководящие документы. М., ФСТК, 2006 г.

6.5. Интернет-ресурсы

21. http://www.rzi.tusur.ru/component/option,com_weblinks/task,view/catid,2/id,33/ сайт ФСБ
22. http://www.topsbi.com/default.asp?trID=161 сайт ФСТЭК России
23. catalog.sec.ru/firms.cfm?fid=7605 билиотека информационных ресурсов по безопасности
24. http://www.uecs.ru/ - Управление экономическими системами
25. http://www.itsec.ru/articles2/allpubliks Портал «Информационная безопасность»: новости, публикации, инновации

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для обеспечения обучения студентов по дисциплине «Защита информации в организационных структурах» Академия располагает следующей материально-технической базой:

- помещениями для проведения семинарских и практических занятий, оборудованными учебной мебелью;
- библиотеку, имеющую рабочие места для студентов, оснащенные компьютерами с доступом к базам данных и сети Интернет;
- компьютерными классами.

Информационные технологии, программное обеспечение и справочные системы

1. www.nnir.ru / - Российская национальная библиотека
2. www.nns.ru / -Национальная электронная библиотека
3. www.rsi.ru / - Российская государственная библиотека
4. www.biznes-karta.ru / -Агентство деловой информации «Бизнес-карта»
5. www. rbs.ru / - Информационное агентство «РосБизнесКонсалтинг»
6. www.rambler.ru / - Поисковая система

7. www.yandex.ru / - Поисковая система
8. www.businеslearning.ru / - Система дистанционного бизнес образования
9. www.test.specialist.ru / - Центр компьютерного обучения МГТУ им. Н. Э. Баумана
10. http://www.consultant.ru/ - Консультант плюс
11. http://www.garant.ru/ - Гарант
12. www.yandex.ru / - Поисковая система
13. www.businеslearning.ru / - Система дистанционного бизнес образования
14. www.test.specialist.ru / - Центр компьютерного обучения МГТУ им. Н. Э. Баумана
15. http://www.consultant.ru/ - Консультант плюс
16. http://www.garant.ru/ - Гарант