

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.О.21 Основы управления информационной безопасностью

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

Автор программы:

Кандидат педагогических наук, доцент Михайлова Елена Михайловна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	4
3. Объем и содержание дисциплины.....	4
4. Контроль знаний обучающихся и типовые оценочные средства.....	15
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	28
6. Учебно-методическое и информационное обеспечение дисциплины.....	29
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	30

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	Проводит анализ и реализует политику управления доступом в компьютерных системах

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Основы управления информационной безопасностью» изучается в 7 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	108
Контактная работа	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	44
Зачет	-

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.	Формы текущего контроля
--------	-----------------------	--------------------------	-------------------------

		Лек ции	Лаб · раб.	СР	
		О	О	О	
7 семестр					
1	Система управления информационной безопасностью организации.	6	4	6	Тестирование
2	Технология управления информационной безопасностью	4	6	6	Тестирование
3	Инциденты информационной безопасности	6	2	6	Тестирование
4	Управление информационными рисками.	4	4	8	Тестирование
5	Управление профилями защиты.	4	8	8	Тестирование
6	Мониторинг и контроль защитных мер.	8	8	10	Выполнение практической работы

Тема 1. Система управления информационной безопасностью организации. (ОПК-1.1)

Лекция.

Базовые определения и основные модели систем. Понятия, характеризующие строение и функционирование систем. Общая классификация систем. Основные закономерности систем. Классификация систем защиты информации, сферы действия. Структура системы защиты информации, назначение составных частей системы. Требования к системам защиты информации.

Лабораторные работы.

1. Что такое ISM?

а. процесс, который обеспечивает конфиденциальность, целостность и доступность активов, информации, данных и услуг организации.+

б. Процесс управления информацией

в. Протокол передачи данных

2. Что является основной целью ISM?

а. Обеспечение эффективного управления информационной безопасностью всех услуг и деятельности в рамках Управления услуг.+

б. Затрудняюсь ответить.

в. Обеспечение отсутствия либо изменения информации и осуществления доступа только преднамеренно субъектами, имеющими на него право.

3. Процесс ISM должен включать в себя (несколько вариантов):

а. формирование, управление, распространение и соблюдение Политики информационной безопасности и других вспомогательных политик, которые имеют отношение к информационной безопасности. Политика информационной безопасности (SecurityPolicy) - политика, определяющая подход организации к управлению информационной безопасностью+

б. понимание согласованных текущих и будущих требований бизнеса к безопасности;+

в. использование контролей безопасности для выполнения Политики информационной безопасности и управления рисками, связанными с доступом к информации, системам и услугам. Термин "контроль безопасности" является заимствованным из английского языка и в данном контексте означает набор контрмер и мер предосторожности, применяемых для аннулирования, уменьшения рисков и противостояния им. То есть контроль безопасности состоит из проактивных и реактивных действий;+

г. документирование перечня контролей безопасности, действий по их эксплуатации и управлению, а также всех связанных с ними рисков;+

4. Ключевые деятельности в рамках ISM (несколько вариантов):

а. формирование, пересмотр и корректирование Политики информационной безопасности и набора поддерживающих ее вспомогательных политик;+

б. реализация и соблюдение политик информационной безопасности, а также обеспечение взаимодействия между ними;+

в. оценка и классификация всех информационных активов и документов;+

г. анализ расписания

5. В качестве ключевых показателей производительности процесса Управления информационной безопасностью можно использовать (несколько вариантов):

а. отсутствие политики безопасности

б. процентное уменьшение негативного влияния на бизнес со стороны "брешей" и инцидентов;+

в. количество предложенных улучшений в отношении контролей и процедур;+

6. Что НЕ является процедурой внедрения системы управления информационной безопасности:

а. внедрение мер по снижению информационных рисков

б. определение методов оценки эффективности внедренных мер

в. повышение квалификации сотрудников компании в области ИБ

г. выбор мер по снижению информационных рисков+

д. внедрение системы управления инцидентами ИБ

7. Какой стандарт устанавливает требования к системе управления информационной безопасностью предприятия?

а. ISO/IEC 27002:2007

б. ISO/IEC 27001:2003

в. ISO/IEC 27001:2005+

г. ISO/IEC 27005:2001

8. Модель системы информационной безопасности предприятия это?

а. совокупность внешних и внутренних факторов, их влияние на состояние информационной безопасности предприятия и обеспечение сохранности ресурсов.+

б. риски, отражающие предполагаемый ущерб в результате реализации угрозы информационной безопасности.

9. Источниками внешних угроз являются (несколько вариантов):

а. деятельность конкурентов по перехвату важной информации;+

б. преднамеренные действия по разрушению, уничтожению или модификации информации;+

в. отсутствие координации деятельности подразделений предприятия в сфере защиты информации;

г. преднамеренные действия персонала по уничтожению или модификации информации;

10. К источникам внутренних угроз относятся (несколько вариантов) :

а. непреднамеренные ошибки персонала, отказы технических средств и сбои в информационных системах;

б. нарушения установленных регламентов сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации.

в. непреднамеренные действия сотрудников сторонних организаций, повлекшие за собой отказ в работе элементов системы;+

г. стихийные бедствия и катастрофы, аварии, экстремальные ситуации.+

Задания для самостоятельной работы.

1. Объект, предмет и задачи науки криминалистики, ее методы.
2. Система науки криминалистики; место криминалистики в системе наук.
3. Основные этапы формирования криминалистики как самостоятельной отрасли знания.
4. Развитие криминалистики в зарубежных странах.

Тема 2. Технология управления информационной безопасностью (ОПК-1.1)

Лекция.

Состав и содержание управленческих функций. Технология управления службой информационной безопасности. Значение управленческих решений. Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Методы и формы контроля выполнения планов. Критерии эффективности службы информационной безопасности. Пути и способы повышения эффективности управления службой информационной безопасности.

Лабораторные работы.

1. Кто является основным ответственным за определение уровня классификации информации?
 - А. Руководитель среднего звена
 - Б. Высшее руководство
 - В. Владелец+
 - Г. Пользователь
2. Эффективная программа безопасности требует сбалансированного применения:
 - А. Технических и нетехнических методов+
 - Б. Контрмер и защитных механизмов
 - В. Физической безопасности и технических средств защиты
 - Г. Процедур безопасности и шифрования
3. Что из перечисленного не является целью проведения анализа рисков?
 - А. Делегирование полномочий+
 - Б. Количественная оценка воздействия потенциальных угроз
 - В. Выявление рисков
 - Г. Определение баланса между воздействием риска и стоимостью необходимых контрмер
4. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
 - А. Чтобы убедиться, что проводится справедливая оценка
 - Б. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
 - В. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа+
 - Г. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку
5. Аудит информационной безопасности представляет собой:
 - А. проверку выполнения требований законодательства по защите сведений, составляющих коммерческую тайну
 - Б. оценку мер по защите информационных ресурсов+
 - В. проверку выполнения требований государственных стандартов в сфере информационной безопасности
6. Сертификация системы безопасности на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:
 - А. внешнего аудита+
 - Б. внутреннего аудита
 - В. инструментальной проверки защищенности

7. В электронных справочных системах, используемых для управления информационной безопасностью, содержатся:

- А. типовые регламенты аудита информационной безопасности
- Б. типовая документация на системы защиты информации
- В. типовые политики безопасности+

8. В определении задач менеджмента в сфере информационной безопасности фигурируют такие понятия как (несколько вариантов):

- А. комплексность+
- Б. целостность
- В. нейтральность
- Г. непрерывность+

9. Услуги внешних аудиторов используются для (несколько вариантов):

- А. снижения затрат на аудит
- Б. повышения объективности аудита+
- В. получения сертификатов на соответствие определенным стандартам+

10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- А. Сотрудники+
- Б. Хакеры
- В. Атакующие
- Г. Контрагенты

Задания для самостоятельной работы.

1. Понятие и научные основы криминалистической идентификации.
2. Объекты, субъекты и виды криминалистической идентификации.
3. Процесс идентификации и этапы идентификационного исследования.
4. Криминалистическая диагностика: понятие и значение.
5. Диагностические задачи и этапы их решения в ходе диагностического исследования.

Тема 3. Инциденты информационной безопасности (ОПК-1.1)

Лекция.

Понятие инцидента информационной безопасности. Методы и средства обнаружения и реагирования на инциденты информационной безопасности. Порядок расследования инцидентов информационной безопасности.

Лабораторные работы.

1. Согласно ГОСТ Р ИСО/МЭК ТО 18044-2007 инцидент информационной безопасности означает:
 - а) Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.+
 - б) Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
 - в) Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов.
 - г) Группу обученных и доверенных членов организации.
2. Для достижения целей в соответствии с пунктом 4.1(ГОСТ Р ИСО/МЭК ТО 18044-2007) менеджмент инцидентов ИБ подразделяют на четыре отдельных этапа. На какие?
 - а) разработка; создание; внедрение; использование.

б) планирование; создание; внедрение; улучшение.

в) планирование и подготовка; использование; анализ; улучшение.+

г) создание; внедрение; анализ; дальнейшее её улучшение.

3. Выберите из списка процессы, которые необходимо осуществить при использовании системы менеджмента инцидентов ИБ (согласно ГОСТ Р ИСО/МЭК ТО 18044-2007)(несколько вариантов ответа):

а) отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы.

б) обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами).+

в) сбор информации, связанной с событиями ИБ, и оценку этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ.+

г) изучить уроки, извлеченные из инцидентов ИБ.

4. Инцидентами информационной безопасности являются (выберите несколько вариантов ответа):

а) утрата услуг, оборудования или устройств.+

б) изменение топологии вычислительных сетей.

в) изменение параметров работы средств защиты информации.

г) системные сбои или перегрузки.+

5. Для устранения последствий и причин инцидента информационной безопасности в организации создаются специальные группы, укажите какие специалисты входят в эту группу(выберите несколько вариантов ответа):

а) специалисты Биологического департамента.

б) специалисты Юридического департамента.+

в) специалисты аттестации объектов информатизации.

г) специалисты Департамента Информационных Технологий.+

6. Найдите ключевые вопросы, которые необходимо рассмотреть для построения оптимальной системы менеджмента инцидентов ИБ (выберите несколько вариантов ответа):

а) конфиденциальность.+

б) обязательства руководства.+

в) анонимность.+

г) обязательства работников.

д) риски ИБ.

7. Из каких частей состоит система криминалистической фотографии (выберите несколько вариантов ответа):

а) судебно – криминалистическая.

б) судебно - экспертная.+

в) судебно – медицинская.

г) судебно - оперативная.+

8. Методы криминалистической фотографии – это:

а) совокупность правил и рекомендаций по выбору фотографических средств, условий съемки и обработки экспонированных изображений для получения фотографических снимков, отвечающих целям и требованиям фиксации и исследования вещественных доказательств.+

б) совокупность правил и рекомендаций по правильному выбору точек съемки, направления и расстояния фотографирования отношении каждого объекта съемки

в) это система специальных методов, приемов и средств съемки, используемых для выявления и фиксации невидимых или слабовидимых объектов и их признаков в процессе проведения экспертиз.

г) фотографирование места проведения следственного (розыскной) действия на фоне окружающей его обстановки.

9. Криминалистическую фотографию подразделяют на (выберите несколько вариантов ответа):

а) судебно – следственную.+

б) судебно – розыскную.

в) судебно – медицинскую.

г) оперативную. +

д) судебно – экспертную. +

10. Что первым указывается при оформлении фототаблиц:

а) Указывается адрес и время преступления.

б) Указывается, к примеру, «Фото № 1: Ориентирующая съёмка. Место причинения тяжких телесных повреждений, по адресу: ул. Советская 111 г. Тамбова».

в) Указывается государственный орган, сотрудник которого осуществляет фотосъёмку, и по какому факту фотосъёмка осуществляется. +

г) Указывается общая информация.

Задания для самостоятельной работы.

1. Предмет и задачи криминалистической техники, ее система.

2. Классификация технико-криминалистических средств и методов.

3. Система и значение криминалистической фотографии.

4. Требования, предъявляемые к процессуальному оформлению результатов применения средств фотосъёмки, звуко- и видеозаписи.

Тема 4. Управление информационными рисками. (ОПК-1.1)

Лекция.

Цели управления информационными рисками. Процесс управления информационными рисками. Алгоритм управления информационными рисками. Принятие решений в условиях определенности, риска и неопределенности. Способы снижения информационного риска.

Лабораторные работы.

1) Управление информационными рисками — это...

а) важная часть менеджмента всей организации, обеспечивающая эффективность процессов и решающая не только тактические, но и стратегические задачи

б) комплекс мероприятий по объективной идентификации и оценке наиболее важных для компании информационных процессов, степени их защищенности и контроля +

в) циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации

г) набор параметров обеспечивает защиту компьютеров

2) Риск является функцией (несколько вариантов):

а) размера возможного ущерба +

б) числа уязвимостей в системе

в) уставного капитала организации

г) вероятности реализации угрозы +

3) Уровень риска является функцией:

а) вероятности реализации угрозы +

б) стоимости защитных средств

в) числа уязвимостей в системе

г) уставного капитала организации

4) В число возможных стратегий нейтрализации рисков входят (несколько вариантов):

а) ликвидация риска +

б) игнорирование риска

в) принятие риска +

г) сокрытие риска

5) В число этапов управления рисками входят (несколько вариантов):

а) анализ угроз +

б) угрозы проведения анализа

в) выявление уязвимых мест +

- г) наказание за создание уязвимостей
- б) Первый шаг в анализе угроз - это:
 - а) идентификация угроз +
 - б) аутентификация угроз
 - в) ликвидация угроз
 - г) минимизация угроз
- 7) После идентификации угрозы необходимо оценить (несколько вариантов):
 - а) вероятность ее осуществления +
 - б) ущерб от ее осуществления +
 - в) частоту ее осуществления
 - г) способ её ликвидации
- 8) При анализе стоимости защитных мер следует учитывать (несколько вариантов):
 - а) расходы на закупку оборудования +
 - б) расходы на закупку программ +
 - в) расходы на обучение персонала +
 - г) количество защитных мер
- 9) Управление рисками включает в себя следующие виды деятельности (несколько вариантов):
 - а) оценка рисков +
 - б) выбор защитных средств +
 - в) ликвидация источников угроз
 - г) определение ответственных за анализ рисков
- 10) Оценка рисков позволяет ответить на следующие вопросы:
 - а) как спроектировать надежную защиту?
 - б) какую политику безопасности предпочесть?
 - в) какие защитные средства экономически целесообразно использовать? +
 - г) чем рискуют системные администраторы?
- 11) В чём заключается качественное управление информационными рисками (несколько вариантов):
 - а) определении +
 - б) минимизации +
 - в) затратности
 - г) контроле +
- 12) Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
 - а) Чтобы убедиться, что проводится справедливая оценка
 - б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
 - в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа +
 - г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

Задания для самостоятельной работы.

1. Понятие и научные основы отождествления человека по признакам внешности.
2. Классификация признаков внешности человека.
3. Источники получения информации о внешнем облике человека и способы ее фиксации.
4. Основные правила описания признаков внешности по методу «словесный портрет».
5. Использование компьютерных средств для изготовления субъективных портретов.

Тема 5. Управление профилями защиты. (ОПК-1.1)

Лекция.

Понятие профиля защиты. Структура профилей защиты. Требования к содержанию разделов профиля защиты. Общая схема формирования профиля защиты. Семейство профилей защиты. Практические приемы формирования профиля защиты.

Лабораторные работы.

- 1) Профиль защиты - это...
 - а) важная часть менеджмента всей организации, обеспечивающая эффективность процессов и решающая не только тактические, но и стратегические задачи
 - б) комплекс мероприятий по объективной идентификации и оценке наиболее важных для компании информационных процессов, степени их защищенности и контроля
 - в) циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации
 - г) специальный нормативный документ представляющий собой совокупность задач защиты, функциональных требований, требований адекватности и их обоснование +
- 2) В каком законодательном документе определено понятие профиля защиты?
 - а) ФЗ “О персональных данных”
 - б) ФЗ “Об информации, информационных технологиях и о защите информации”
 - в) ГОСТ “Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий” +
 - г) ФЗ “О безопасности”
- 3) Как называется совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ?
 - а) продукт ИТ +
 - б) изделие ИТ
 - в) система ИТ
 - г) среда безопасности ИТ
- 4) Обобщенным термином для продуктов и систем ИТ является:
 - а) профиль защиты
 - б) профиль безопасности
 - в) изделие ИТ +
 - г) система ИТ
- 5) Какие цели преследует использование профилей защиты (несколько вариантов)?
 - а) стандартизация наборов требований к информационным продуктам +
 - б) повышение уровня безопасности информационной системы
 - в) оценка безопасности +
 - г) проведение сравнительного анализа уровня безопасности различных изделий ИТ +
 - д) повышение уровня безопасности изделия ИТ
- 6) Выберите правильное утверждение относительно профиля защиты (ПЗ).
 - а) ПЗ регламентирует требования безопасности изделий ИТ и способы реализации этих требований
 - б) ПЗ регламентирует способы реализации определенного уровня безопасности изделия ИТ
 - в) ПЗ содержит рекомендации по реализации определенного уровня безопасности изделия ИТ
 - г) ПЗ регламентирует требования безопасности изделий ИТ, но не регламентирует способов реализации этих требований +
- 7) Профиль защиты может применяться (несколько вариантов):
 - а) к одному продукту
 - б) к определенному классу продуктов +
 - в) совокупности продуктов, не образующих информационную технологию
 - г) совокупности продуктов, образующих информационную технологию +

8) Какой подраздел профиля защиты должен давать общую характеристику профилю защиты и иметь описательную форму?

- а) аннотация +
- б) обоснование
- в) среда безопасности
- г) замечания по применению

9) Какой подраздел профиля защиты должен обеспечить маркировку и описательную информацию, необходимые для однозначной идентификации и регистрации профиля защиты?

- а) обоснование
- б) среда безопасности
- в) замечания по применению
- г) идентификация +

10) В каком разделе профиля защиты содержится аннотация и идентификация?

- а) введение +
- б) обоснование
- в) среда безопасности
- г) замечания по применению

11) Когда производится регистрация профиля защиты?

- а) до его создания
- б) после оценки и сертификации +
- в) в процессе эксплуатации
- г) во время создания

12) Как называется совокупность записей (в электронном или электронном и бумажном виде), включающих в себя регистрационные метки, а также связанную с ними дополнительную информацию о профилях защиты?

- а) журнал
- б) реестр +
- в) набор
- г) каталог

13) Из каких частей состоит каждая запись реестра (несколько ответов)?

- а) тип элемента реестра +
- б) год регистрации +
- в) тип регистрации
- г) регистрационный номер +
- д) лицо или организация, выдавшая сертификат соответствия

14) Сколько значений может принимать тип элемента реестра?

- а) 2
- б) 3 +
- в) 4
- г) 5

15) Для профиля защиты с регистрационным номером 5, зарегистрированным 11 февраля 2011 года, запись в реестре будет иметь следующий вид:

- а) ПД-2011-02
- б) ПЗ-02-2011-005
- в) ПЗ-2011-005 +
- г) ПЗ-02-2011

Задания для самостоятельной работы.

1. Классификация материальных следов, правила их обнаружения, фиксации и изъятия.
2. Следы рук (дактилоскопия).

3. Следы ног.
4. Следы орудий взлома, инструментов, механизмов и возможности их криминалистического исследования.
5. Следы транспортных средств.

Тема 6. Мониторинг и контроль защитных мер. (ОПК-1.1)

Лекция.

Понятие мониторинга и контроля защитных мер. Самооценка информационной безопасности. Оценка менеджмента информационной безопасности организации.

Лабораторные работы.

«Построение концепции информационной безопасности предприятия»

Цель работы

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – Концепции и Политики информационной безопасности. Если Концепция ИБ в общих чертах определяет, ЧТО необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит КАК, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

принятия обоснованных управленческих решений по разработке мер защиты информации;
выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности.

3. Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

Классификации угроз.

Основные непреднамеренные искусственные угрозы.

Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

Задачи организационного обеспечения информационной безопасности.

Подразделения, занятые в обеспечении информационной безопасности.

Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

Общие положения.

Защита информационных ресурсов от несанкционированного доступа.

Средства комплексной защиты от потенциальных угроз.

Обеспечение качества в системе безопасности.

Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

Правовое обеспечение юридических отношений с работниками Предприятия .

Правовое обеспечение юридических отношений с партнерами Предприятия.

Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

4. Содержание отчета

Титульный лист

Содержание

Задание

Концепция ИБ заданного предприятия по плану, приведенному в задании

Задания для самостоятельной работы.

1. Общие положения криминалистической баллистики.

2. Классификация и характеристики огнестрельного оружия.

3. Обнаружение, осмотр, фиксация, изъятие огнестрельного оружия и следов его применения.

4. Понятие и классификация холодного оружия

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

7 семестр

- посещаемость – 10 баллов
- текущий контроль – 60 баллов
- контрольные срезы – 2 среза по 15 баллов каждый
- премиальные баллы – 10 баллов

Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки

1.	Система управления информационной безопасностью организации.	Тестирование	15	Тест состоит из вопросов с выбором ответа. 15 баллов - студент правильно отвечает более чем на 90% вопросов. 6-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-5 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
2.	Технология управления информационной безопасностью	Тестирование(контрольный срез)	15	Тест состоит из вопросов с выбором ответа. 15 баллов - студент правильно отвечает более чем на 90% вопросов. 6-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-5 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
3.	Инциденты информационной безопасности	Тестирование	15	Тест состоит из вопросов с выбором ответа. 15 баллов - студент правильно отвечает более чем на 90% вопросов. 6-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-5 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
4.	Управление информационными рисками.	Тестирование	15	Тест состоит из вопросов с выбором ответа. 15 баллов - студент правильно отвечает более чем на 90% вопросов. 6-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-5 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
5.	Управление профилями защиты.	Тестирование(контрольный срез)	15	Тест состоит из вопросов с выбором ответа. 15 баллов - студент правильно отвечает более чем на 90% вопросов. 6-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-5 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
6.	Мониторинг и контроль защитных мер.	Выполнение практической работы	15	Лабораторные работы выполняются по тематике практических занятий. 15 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 5 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
7.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7-5 баллов – посещаемость студента составляет не менее 80 % занятий 3 баллов – посещаемость студента составляет не менее 50 % занятий 1 балла – посещаемость студента составляет не менее 25 % занятий

8.	Премияльные баллы	10	Дополнительные премияльные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
9.	Итого за семестр	100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

4.2 Типовые оценочные средства текущего контроля

Выполнение практической работы

Тема 6. Мониторинг и контроль защитных мер.

«Построение концепции информационной безопасности предприятия»

Цель работы

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – Концепции и Политики информационной безопасности. Если Концепция ИБ в общих чертах определяет, ЧТО необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит КАК, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

принятия обоснованных управленческих решений по разработке мер защиты информации;
выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности.

3. Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

Классификации угроз.

Основные непреднамеренные искусственные угрозы.

Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

Задачи организационного обеспечения информационной безопасности.

Подразделения, занятые в обеспечении информационной безопасности.

Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

Общие положения.

Защита информационных ресурсов от несанкционированного доступа.

Средства комплексной защиты от потенциальных угроз.

Обеспечение качества в системе безопасности.

Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

Правовое обеспечение юридических отношений с работниками Предприятия .

Правовое обеспечение юридических отношений с партнерами Предприятия.

Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

4. Содержание отчета

Титульный лист

Содержание

Задание

Концепция ИБ заданного предприятия по плану, приведенному в задании

Тестирование

Тема 1. Система управления информационной безопасностью организации.

1. Что такое ISM?

а. процесс, который обеспечивает конфиденциальность, целостность и доступность активов, информации, данных и услуг организации.+

б. Процесс управления информацией

в. Протокол передачи данных

2. Что является основной целью ISM?

а. Обеспечение эффективного управления информационной безопасностью всех услуг и деятельности в рамках Управления услуг.+

б. Затрудняюсь ответить.

в. Обеспечение отсутствия либо изменения информации и осуществления доступа только преднамеренно субъектами, имеющими на него право.

3. Процесс ISM должен включать в себя (несколько вариантов):

а. формирование, управление, распространение и соблюдение Политики информационной безопасности и других вспомогательных политик, которые имеют отношение к информационной безопасности. Политика информационной безопасности (SecurityPolicy) - политика, определяющая подход организации к управлению информационной безопасностью+

б. понимание согласованных текущих и будущих требований бизнеса к безопасности;+

в. использование контролей безопасности для выполнения Политики информационной безопасности и управления рисками, связанными с доступом к информации, системам и услугам. Термин "контроль безопасности" является заимствованным из английского языка и в данном контексте означает набор контрмер и мер предосторожности, применяемых для аннулирования, уменьшения рисков и противостояния им. То есть контроль безопасности состоит из проактивных и реактивных действий;+

г. документирование перечня контролей безопасности, действий по их эксплуатации и управлению, а также всех связанных с ними рисков;+

4. Ключевые деятельности в рамках ISM (несколько вариантов):

а. формирование, пересмотр и корректирование Политики информационной безопасности и набора поддерживающих ее вспомогательных политик;+

б. реализация и соблюдение политик информационной безопасности, а также обеспечение взаимодействия между ними;+

в. оценка и классификация всех информационных активов и документов;+

г. анализ расписания

5. В качестве ключевых показателей производительности процесса Управления информационной безопасностью можно использовать (несколько вариантов):

а. отсутствие политики безопасности

б. процентное уменьшение негативного влияния на бизнес со стороны "брешей" и инцидентов;+

в. количество предложенных улучшений в отношении контролей и процедур;+

6. Что НЕ является процедурой внедрения системы управления информационной безопасности:

а. внедрение мер по снижению информационных рисков

б. определение методов оценки эффективности внедренных мер

в. повышение квалификации сотрудников компании в области ИБ

г. выбор мер по снижению информационных рисков+

д. внедрение системы управления инцидентами ИБ

7. Какой стандарт устанавливает требования к системе управления информационной безопасностью предприятия?

а. ISO/NEC 27002:2007

б. ISO/NEC 27001:2003

в. ISO/NEC 27001:2005+

г. ISO/NEC 27005:2001

8. Модель системы информационной безопасности предприятия это?

а. совокупность внешних и внутренних факторов, их влияние на состояние информационной безопасности предприятия и обеспечение сохранности ресурсов.+

б. риски, отражающие предполагаемый ущерб в результате реализации угрозы информационной безопасности.

9. Источниками внешних угроз являются (несколько вариантов):

- а. деятельность конкурентов по перехвату важной информации;+
- б. преднамеренные действия по разрушению, уничтожению или модификации информации;+
- в. отсутствие координации деятельности подразделений предприятия в сфере защиты информации;
- г. преднамеренные действия персонала по уничтожению или модификации информации;

10. К источникам внутренних угроз относятся (несколько вариантов) :

- а. непреднамеренные ошибки персонала, отказы технических средств и сбои в информационных системах;
- б. нарушения установленных регламентов сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации.
- в. непреднамеренные действия сотрудников сторонних организаций, повлекшие за собой отказ в работе элементов системы;+
- г. стихийные бедствия и катастрофы, аварии, экстремальные ситуации.+

Тема 2. Технология управления информационной безопасностью

1. Кто является основным ответственным за определение уровня классификации информации?

- А. Руководитель среднего звена
- Б. Высшее руководство
- В. Владелец+
- Г. Пользователь

2. Эффективная программа безопасности требует сбалансированного применения:

- А. Технических и нетехнических методов+
- Б. Контрмер и защитных механизмов
- В. Физической безопасности и технических средств защиты
- Г. Процедур безопасности и шифрования

3. Что из перечисленного не является целью проведения анализа рисков?

- А. Делегирование полномочий+
 - Б. Количественная оценка воздействия потенциальных угроз
 - В. Выявление рисков
 - Г. Определение баланса между воздействием риска и стоимостью необходимых контрмер
4. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
- А. Чтобы убедиться, что проводится справедливая оценка
 - Б. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
 - В. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа+
 - Г. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

5. Аудит информационной безопасности представляет собой:

- А. проверку выполнения требований законодательства по защите сведений, составляющих коммерческую тайну
- Б. оценку мер по защите информационных ресурсов+
- В. проверку выполнения требований государственных стандартов в сфере информационной безопасности

6. Сертификация системы безопасности на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:

- А. внешнего аудита+
 - Б. внутреннего аудита
 - В. инструментальной проверки защищенности
7. В электронных справочных системах, используемых для управления информационной безопасностью, содержатся:
- А. типовые регламенты аудита информационной безопасности
 - Б. типовая документация на системы защиты информации
 - В. типовые политики безопасности+
8. В определении задач менеджмента в сфере информационной безопасности фигурируют такие понятия как (несколько вариантов):
- А. комплексность+
 - Б. целостность
 - В. нейтральность
 - Г. непрерывность+
9. Услуги внешних аудиторов используются для (несколько вариантов):
- А. снижения затрат на аудит
 - Б. повышения объективности аудита+
 - В. получения сертификатов на соответствие определенным стандартам+
10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
- А. Сотрудники+
 - Б. Хакеры
 - В. Атакующие
 - Г. Контрагенты

Тема 3. Инциденты информационной безопасности

1. Согласно ГОСТ Р ИСО/МЭК ТО 18044-2007 инцидент информационной безопасности означает:
- а) Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.+
 - б) Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
 - в) Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов.
 - г) Группу обученных и доверенных членов организации.
2. Для достижения целей в соответствии с пунктом 4.1(ГОСТ Р ИСО/МЭК ТО 18044-2007) менеджмент инцидентов ИБ подразделяют на четыре отдельных этапа. На какие?
- а) разработка; создание; внедрение; использование.
 - б) планирование; создание; внедрение; улучшение.
 - в) планирование и подготовка; использование; анализ; улучшение.+
 - г) создание; внедрение; анализ; дальнейшее её улучшение.
3. Выберите из списка процессы, которые необходимо осуществить при использовании системы менеджмента инцидентов ИБ (согласно ГОСТ Р ИСО/МЭК ТО 18044-2007)(несколько вариантов ответа):
- а) отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы.
 - б) обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами).+
 - в) сбор информации, связанной с событиями ИБ, и оценку этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ.+

г) изучить уроки, извлеченные из инцидентов ИБ.

4. Инцидентами информационной безопасности являются (выберите несколько вариантов ответа):

- а) утрата услуг, оборудования или устройств.+
- б) изменение топологии вычислительных сетей.
- в) изменение параметров работы средств защиты информации.
- г) системные сбои или перегрузки.+

5. Для устранения последствий и причин инцидента информационной безопасности в организации создаются специальные группы, укажите какие специалисты входят в эту группу (выберите несколько вариантов ответа):

- а) специалисты Биологического департамента.
- б) специалисты Юридического департамента.+
- в) специалисты аттестации объектов информатизации.
- г) специалисты Департамента Информационных Технологий.+

6. Найдите ключевые вопросы, которые необходимо рассмотреть для построения оптимальной системы менеджмента инцидентов ИБ (выберите несколько вариантов ответа):

- а) конфиденциальность.+
- б) обязательства руководства.+
- в) анонимность.+
- г) обязательства работников.
- д) риски ИБ.

7. Из каких частей состоит система криминалистической фотографии (выберите несколько вариантов ответа):

- а) судебно – криминалистическая.
- б) судебно - экспертная.+
- в) судебно – медицинская.
- г) судебно - оперативная.+

8. Методы криминалистической фотографии – это:

- а) совокупность правил и рекомендаций по выбору фотографических средств, условий съемки и обработки экспонированных изображений для получения фотографических снимков, отвечающих целям и требованиям фиксации и исследования вещественных доказательств.+
- б) совокупность правил и рекомендаций по правильному выбору точек съемки, направления и расстояния фотографирования отношении каждого объекта съемки
- в) это система специальных методов, приемов и средств съемки, используемых для выявления и фиксации невидимых или слабовидимых объектов и их признаков в процессе проведения экспертиз.
- г) фотографирование места проведения следственного (розыскной) действия на фоне окружающей его обстановки.

9. Криминалистическую фотографию подразделяют на (выберите несколько вариантов ответа):

- а) судебно – следственную.+
- б) судебно – розыскную.
- в) судебно – медицинскую.
- г) оперативную.+
- д) судебно – экспертную.+

10. Что первым указывается при оформлении фототаблиц:

- а) Указывается адрес и время преступления.
- б) Указывается, к примеру, «Фото № 1: Ориентирующая съёмка. Место причинения тяжких телесных повреждений, по адресу: ул. Советская 111 г. Тамбова».
- в) Указывается государственный орган, сотрудник которого осуществляет фотосъёмку, и по какому факту фотосъёмка осуществляется.+
- г) Указывается общая информация.

Тема 4. Управление информационными рисками.

1) Управление информационными рисками — это...

- а) важная часть менеджмента всей организации, обеспечивающая эффективность процессов и решающая не только тактические, но и стратегические задачи
- б) комплекс мероприятий по объективной идентификации и оценке наиболее важных для компании информационных процессов, степени их защищенности и контроля +
- в) циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации
- г) набор параметров обеспечивает защиту компьютеров

2) Риск является функцией (несколько вариантов):

- а) размера возможного ущерба +
- б) числа уязвимостей в системе
- в) уставного капитала организации
- г) вероятности реализации угрозы +

3) Уровень риска является функцией:

- а) вероятности реализации угрозы +
- б) стоимости защитных средств
- в) числа уязвимостей в системе
- г) уставного капитала организации

4) В число возможных стратегий нейтрализации рисков входят (несколько вариантов):

- а) ликвидация риска +
- б) игнорирование риска
- в) принятие риска +
- г) сокрытие риска

5) В число этапов управления рисками входят (несколько вариантов):

- а) анализ угроз +
- б) угрозы проведения анализа
- в) выявление уязвимых мест +
- г) наказание за создание уязвимостей

6) Первый шаг в анализе угроз - это:

- а) идентификация угроз +
- б) аутентификация угроз
- в) ликвидация угроз
- г) минимизация угроз

7) После идентификации угрозы необходимо оценить (несколько вариантов):

- а) вероятность ее осуществления +
- б) ущерб от ее осуществления +
- в) частоту ее осуществления
- г) способ её ликвидации

8) При анализе стоимости защитных мер следует учитывать (несколько вариантов):

- а) расходы на закупку оборудования +
- б) расходы на закупку программ +
- в) расходы на обучение персонала +
- г) количество защитных мер

9) Управление рисками включает в себя следующие виды деятельности (несколько вариантов):

- а) оценка рисков +
- б) выбор защитных средств +
- в) ликвидация источников угроз
- г) определение ответственных за анализ рисков

10) Оценка рисков позволяет ответить на следующие вопросы:

- а) как спроектировать надежную защиту?
- б) какую политику безопасности предпочесть?
- в) какие защитные средства экономически целесообразно использовать? +
- г) чем рискуют системные администраторы?

11) В чём заключается качественное управление информационными рисками (несколько вариантов):

- а) определении +
- б) минимизации +
- в) затратности
- г) контроле +

12) Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- а) Чтобы убедиться, что проводится справедливая оценка
- б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа +
- г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

Тема 5. Управление профилями защиты.

1) Профиль защиты - это...

- а) важная часть менеджмента всей организации, обеспечивающая эффективность процессов и решающая не только тактические, но и стратегические задачи
- б) комплекс мероприятий по объективной идентификации и оценке наиболее важных для компании информационных процессов, степени их защищенности и контроля
- в) циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации
- г) специальный нормативный документ представляющий собой совокупность задач защиты, функциональных требований, требований адекватности и их обоснование +

2) В каком законодательном документе определено понятие профиля защиты?

- а) ФЗ “О персональных данных”
- б) ФЗ “Об информации, информационных технологиях и о защите информации”
- в) ГОСТ “Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий” +
- г) ФЗ “О безопасности”

3) Как называется совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ?

- а) продукт ИТ +
- б) изделие ИТ
- в) система ИТ
- г) среда безопасности ИТ

4) Обобщенным термином для продуктов и систем ИТ является:

- а) профиль защиты
- б) профиль безопасности
- в) изделие ИТ +
- г) система ИТ

5) Какие цели преследует использование профилей защиты (несколько вариантов)?

- а) стандартизация наборов требований к информационным продуктам +
 - б) повышение уровня безопасности информационной системы
 - в) оценка безопасности +
 - г) проведение сравнительного анализа уровня безопасности различных изделий ИТ +
 - д) повышение уровня безопасности изделия ИТ
- 6) Выберите правильное утверждение относительно профиля защиты (ПЗ).
- а) ПЗ регламентирует требования безопасности изделий ИТ и способы реализации этих требований
 - б) ПЗ регламентирует способы реализации определенного уровня безопасности изделия ИТ
 - в) ПЗ содержит рекомендации по реализации определенного уровня безопасности изделия ИТ
 - г) ПЗ регламентирует требования безопасности изделий ИТ, но не регламентирует способов реализации этих требований+
- 7) Профиль защиты может применяться (несколько вариантов):
- а) к одному продукту
 - б) к определенному классу продуктов +
 - в) совокупности продуктов, не образующих информационную технологию
 - г) совокупности продуктов, образующих информационную технологию+
- 8) Какой подраздел профиля защиты должен давать общую характеристику профилю защиты и иметь описательную форму?
- а) аннотация +
 - б) обоснование
 - в) среда безопасности
 - г) замечания по применению
- 9) Какой подраздел профиля защиты должен обеспечить маркировку и описательную информацию, необходимые для однозначной идентификации и регистрации профиля защиты?
- а) обоснование
 - б) среда безопасности
 - в) замечания по применению
 - г) идентификация +
- 10) В каком разделе профиля защиты содержится аннотация и идентификация?
- а) введение +
 - б) обоснование
 - в) среда безопасности
 - г) замечания по применению
- 11) Когда производится регистрация профиля защиты?
- а) до его создания
 - б) после оценки и сертификации +
 - в) в процессе эксплуатации
 - г) во время создания
- 12) Как называется совокупность записей (в электронном или электронном и бумажном виде), включающих в себя регистрационные метки, а также связанную с ними дополнительную информацию о профилях защиты?
- а) журнал
 - б) реестр +
 - в) набор
 - г) каталог
- 13) Из каких частей состоит каждая запись реестра (несколько ответов)?
- а) тип элемента реестра +
 - б) год регистрации +
 - в) тип регистрации

- г) регистрационный номер +
 - д) лицо или организация, выдавшая сертификат соответствия
- 14) Сколько значений может принимать тип элемента реестра?

- а) 2
- б) 3 +
- в) 4
- г) 5

15) Для профиля защиты с регистрационным номером 5, зарегистрированным 11 февраля 2011 года, запись в реестре будет иметь следующий вид:

- а) ПД-2011-02
- б) ПЗ-02-2011-005
- в) ПЗ-2011-005 +
- г) ПЗ-02-2011

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ОПК-1.1)

1. Внутренняя мотивация к обеспечению ИБ на предприятии.
2. Бизнес-модель предприятия. Информационные потоки.
3. Документы 1го уровня: стратегия информационной безопасности, политика информационной безопасности
4. Задачи различных подразделений по обеспечению ИБ
5. Процессы обеспечения информационной безопасности.
6. Контроль качества процессов информационной безопасности.
7. Система управления информационной безопасностью предприятия.

Типовые задания для зачета (ОПК-1.1)

1. Выберите функции управления
 - а) Планирование
 - б) Организация
 - в) Мотивация
 - г) Развитие
 - д) Контроль
- 2 Методы анализа конфликт логических данных:
 - а) статистический метод;
 - б) математический метод;
 - в) системно-экспертный метод;
 - г) исторический анализ;
 - д) компаративный анализ.
- 3 Выбрать стадии реализации системы управления информационной безопасностью:
 - а) формирование политики в области рисков.
 - б) анализ бизнес-процессов.
 - в) согласование рисков с экспертами

г) анализ рисков.

д) формирование целевой концепции.

4. Какие пункты включает «Замкнутый жизненный цикл системы управления информационной безопасностью»

а) Аудит СУИБ

б) Корректировка мер по минимизации рисков ИБ

в) планирование мер по минимизации рисков ИБ

г) согласование запланированных мер д) проверка

5. СУИБ включает в себя:

а) организационную структуру,

б) политики,

в) распределение прав и обязанностей,

г) осуществление на практике,

д) процессы и ресурсы

6. Назовите методы управления информационной безопасности

а) административные

б) инженерно-технические

в) правовые

г) теоретические

д) экономические

е) социально-педагогические

7. Типы мотивов в коллективе

а) мотив как внутренне осознанные потребности;

б) мотив как внешняя осознанная потребность;

в) мотив как инструмент удовлетворения потребности

г) мотив как намерение, побуждающее поведение;

8. Мероприятия для обеспечения защиты информации в автоматизированной системе управления

а) формирование требований к защите информации в автоматизированной системе управления;

б) разработка системы защиты автоматизированной системы управления;

в) согласование системы защиты автоматизированной системы управления и ввод ее в действие;

г) обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления;

д) обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления.

9 Разработка системы защиты автоматизированной системы управления включает

а) проектирование системы защиты автоматизированной системы управления;

б) согласование системы защиты автоматизированной системы управления

в) разработку эксплуатационной документации на систему защиты автоматизированной системы управления.

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ОПК-1.1	Демонстрирует высокий уровень знаний по основам управления информационной безопасности, обеспечения требуемого качества политики ИБ. Умеет разрабатывать и реализовывать политики управления доступом в компьютерных системах на основе организационных, программно-аппаратных и технических средств защиты информации.

«не зачтено» (0 - 49 баллов)	ОПК-1.1	Не способен продемонстрировать знания по основам управления информационной безопасности, обеспечения требуемого качества политики ИБ. Не умеет разрабатывать и реализовывать политики управления доступом в компьютерных системах на основе организационных, программно-аппаратных и технических средств защиты информации.
---------------------------------	---------	--

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Передков В.М., Митрошкин А.Г. Информационная безопасность и защита информации. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=362895>
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
3. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>
4. Петренко В. И. Теоретические основы защиты информации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015. - 222 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>

6.3 Иные источники:

1. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
2. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Консультант Плюс

Google Chrome

Microsoft Windows 10

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>

5. Российская государственная библиотека. – URL: <https://www.rsl.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prlib.ru>
8. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.