год начала подготовки 2018

АНО ВО «Российский новый университет»

Елецкий филиал Автономной некоммерческой организации высшего образования «Российский новый университет»
(Елецкий филиал АНО ВО «Российский новый университет»)

кафедра прикладной экономики и сферы обслуживания

Рабочая программа учебной дисциплины (модуля)

Информационная безопасность
(наименование учебной дисциплины (модуля))

09.03.03 Прикладная информатика
(код и направление подготовки/специальности)

Прикладная информатика в экономике
(код и направление подготовки/специальности, в случаях, если программа разработана для разных направлений подготовки/специальностей)

Рабочая программа учебной дисциплины (модуля) рассмотрена и утверждена на заседании кафедры 12 февраля 2018 г., протокол № 6.

Заведующий кафедрой Прикладной экономики и сферы обслуживания
(название кафедры)
к.п.н., доцент Гнездилова Н.А. _____
(ученая степень, ученое звание, фамилия и инициалы, подпись заведующего кафедрой)

Елец
2018 год

год начала подготовки 2018

1. НАИМЕНОВАНИЕ И ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Информационная безопасность» является:

Обеспечение профессионального образования, способствующего социальной, академической мобильности, востребованности на рынке труда, успешной карьере, сотрудничеству.

Формирование у обучающихся систематизированных профессионально значимых знаний по информационной безопасности и профессиональных умений и навыков, необходимых бакалавру прикладной информатики в экономике.

Изучение учебной дисциплины направлено на получение общих сведений о предмете информационная безопасность и умение применять основные совокупности методов информационной безопасности, позволяющие обеспечить защиту информации на всех уровнях в современных условиях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП БАКАЛАВРИАТА

Учебная дисциплина «Информационная безопасность» относится к вариативной части дисциплин по выбору учебного плана (Б1.В.15).

Содержание учебной дисциплины тесно связано с логикой и содержанием других изучаемых дисциплин:

Учебная дисциплина содержательно и логически связана с другими учебными дисциплинами, изучаемыми студентами:

- предшествуют освоению данной дисциплины: «Информатика и программирование», «Вычислительные системы, сети и телекоммуникации», «Проектирование информационных систем», «Операционные системы», «Программная инженерия», «Базы данных».
- после изучения данной дисциплины изучаются: «Предметно-ориентированные экономические и информационные системы», «Системы электронной коммерции», «Управление информационными системами».

Дисциплина изучается на заочной форме обучения на 3 курсе в 5, 6 семестрах.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОП

В результате освоения дисциплины обучающийся должен овладеть следующими компетенциями:

ПК-1 Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.

Планируемые результаты освоения компетенций

Компетенция	Показатели (планируемые) результаты обучения
ПК-1 Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.	**Владеть:** - способностью формировать требования к информационной системе в процессе обследования организации и выявления информационной потребности пользователей В1(ПК-1); - методами проектирования информационных систем, стадии и этапы процесса проектирования с учетом выявленных информационных потребностей пользователей обследованной организации В2(ПК-1); - технологией осуществлять содержательное описание бизнес-процесса организации в терминах предметной области с учетом социально-культурных явлений и процессов В3(ПК-1); - навыками постановки целей и задач имитационного моделирования бизнес-процессов организации В4(ПК-1).
	Уметь: - проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе У1(ПК-1);

	- собирать и систематизировать информацию о структуре организации и ее бизнес-процессах в рамках информационной безопасности и безопасности жизнедеятельности пользователей организации У2(ПК-1); - осуществлять содержательное описание бизнес-процесса организации в терминах предметной области с учетом социально-культурных явлений и процессов У3(ПК-1); - выявлять внешние и внутренние случайные факторы, влияющие на бизнес-процессы предприятия с целью раскрытия информационных потребностей пользователей и формирования требования к информационной системе организации У4(ПК-1).
	Знать: - виды и формы процесса обследования организаций, выявления информационных потребностей пользователей и формирование требований к информационной системе З1(ПК-1); - основные понятия информационного менеджмента, маркетинга, теории систем и системного анализа, теории экономических, предметно-ориентированных, корпоративных, интеллектуальных информационных систем, систем электронной коммерции, информационной безопасности в рамках обследования организации З2(ПК-1); - принципы проектирования информационных систем, стадии и этапы процесса проектирования с учетом выявленных информационных потребностей пользователей обследованной организации З3(ПК-1); - сущность методологии имитационного моделирования бизнес-процессов сложных систем с учетом выявленных информационных потребностей пользователей обследованной организации З4(ПК-1).

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Дисциплина предполагает изучение 4 тем. Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

Общий объем учебной дисциплины

№	Форма обучения	Семестр/ сессия, курс	Общая трудоемкость		в том числе контактная работа с преподавателем							СР	Контроль
			в з.е.	в часах	Всего	Л	ПЗ	КоР	зачет	Конс	экзамен		
1.	Заочная	2 сессия, 3 курс	1	36	4	4						32	
		1 сессия, 4 курс	3	108	8		4	1,6		2	0,4	93,4	6,6
	Итого:		4	144	12	4	4	1,6		2	0,4	125,4	6,6

Распределение учебного времени по темам и видам учебных занятий
заочная форма

№	Наименование разделов, тем учебных занятий	Всего часов	Контактная работа с преподавателем							СР	Контроль	Формируемые результаты обучения
			Всего	Л	ПЗ	КоР	зачет	Конс	экзамен			
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
1.	**Модуль 1. Введение в безопасность информации современного предприятия**											

2.	1. Основные понятия, термины и определения в области защиты информации	13	1	1						12		В1(ПК-1) У1(ПК-1) З1(ПК-1) З2(ПК-1)
3.	2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.	13	1	1						12		В1(ПК-1) В2(ПК-1) У1(ПК-1) У2(ПК-1) У4(ПК-1) З1(ПК-1)
4.	3. Законодательная и нормативная база правового регулирования вопросов защиты информации.	14	2	1						12		В2(ПК-1) В3(ПК-1) У3(ПК-1) У4(ПК-1) З2(ПК-1)
5.	4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	15	2	1	1					12		В2(ПК-1) В3(ПК-4) В4(ПК-4) У3(ПК-1) У4(ПК-1) З3(ПК-1) З4(ПК-1)
6.	**Модуль 2. Технологии обеспечения информационной безопасности предприятия**											
7.	5. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	13	1		1					12		В1(ПК-1) В2(ПК-1) У1(ПК-1) У2(ПК-1) У4(ПК-1) З1(ПК-1)
8.	6. Меры и средства защиты информации	13	1							12		В2(ПК-1) В3(ПК-1) У3(ПК-1) У4(ПК-1) З2(ПК-1)
9.	7. Применения криптографических методов защиты информации при работе в сетях.	13	1		1					12		В2(ПК-1) В3(ПК-4) В4(ПК-4) У3(ПК-1) У4(ПК-1) З3(ПК-1) З4(ПК-1)
10.	8. Аудит информационной безопасности	18,4	1		1					17,4		В1(ПК-1) У1(ПК-1) З1(ПК-1) З2(ПК-1)
11.	***Промежуточная аттестация (Экзамен)***	***9,6***				***1,6***		***2***	***0,4***		***6,6***	
12.	**ИТОГО:**	**144**	**12**	**4**	**4**	**1,6**		**2**	**0,4**	**125,4**	**6,6**	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ СТРУКТУРИРОВАННОЕ ПО ТЕМАМ

№ п/п	Наименование раздела, темы учебной дисциплины	Содержание раздела, темы
1	2	3
1. __	Информация и	Необходимость защиты информации. Массовая и

	необходимость ее защиты	конфиденциальная информация. Виды тайн. Информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности страны. Основные законодательные акты и нормативные документы, касающиеся государственной тайны и защиты информации в России. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.
2.	Угрозы информационной безопасности	Понятие угрозы информационной безопасности. Классификация и общий анализ угроз. Три вида возможных нарушений информационной системы. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности. Виды противников или «нарушителей». Понятия о видах вирусов. Реализация угроз. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.
3.	Защита информации	Защита информации от случайных угроз. Защита компьютерных систем от несанкционированного вмешательства. Криптографические методы защиты информации. Шифрование. Основные методы шифрования. Стандарты шифрования. Вредоносные программы. Компьютерные вирусы. Средства защиты от компьютерных вирусов. Профилактика заражения компьютерными вирусами. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.
4.	Стандарты в области защиты информации. Построение защищенных информационных систем	Международные стандарты информационного обмена. Стандарты защищенности информации в компьютерных системах. Критерии оценки безопасности компьютерных систем Министерства обороны США. Документы Гостехкомиссии России по защите информации. Европейские критерии безопасности информационных технологий. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Комплексная система защиты информации (КСЗИ). Основные технологии построения защищенных ЭИС. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.

Планы практических занятий

Тема 1. *Информация и необходимость ее защиты.*

1. Необходимость защиты информации.

2. Массовая и конфиденциальная информация.

3. Виды тайн.

4. Информация как объект права собственности.

5. Информационная безопасность как составляющая национальной безопасности страны.

6. Основные законодательные акты и нормативные документы, касающиеся государственной тайны и защиты информации в России.

Тема 2. *Угрозы информационной безопасности.*

1. Понятие угрозы информационной безопасности.

2. Классификация и общий анализ угроз.

3. Три вида возможных нарушений информационной системы.

4. Случайные угрозы информационной безопасности.

5. Преднамеренные угрозы информационной безопасности.

6. Виды противников или «нарушителей».

7. Понятия о видах вирусов. Реализация угроз.

Тема 3. *Защита информации.*

1. Защита информации от случайных угроз.

2. Защита компьютерных систем от несанкционированного вмешательства.

3. Криптографические методы защиты информации.

4. Шифрование.

5. Основные методы шифрования.

6. Стандарты шифрования.

7. Вредоносные программы.

8. Компьютерные вирусы.

9. Средства защиты от компьютерных вирусов.

10. Профилактика заражения компьютерными вирусами.

11. Анализ способов нарушений информационной безопасности.

12. Использование защищенных компьютерных систем.

Тема 4. *Стандарты в области защиты информации. Построение защищенных информационных систем.*

1. Международные стандарты информационного обмена.

2. Стандарты защищенности информации в компьютерных системах.

3. Критерии оценки безопасности компьютерных систем Министерства обороны США.

4. Документы Гостехкомиссии России по защите информации.

5. Европейские критерии безопасности информационных технологий.

6. Основные положения теории информационной безопасности информационных систем.

7. Модели безопасности и их применение.

8. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

9. Комплексная система защиты информации (КСЗИ).

10. Основные технологии построения защищенных ЭИС.

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Контроль самостоятельной работы студента осуществляется в форме:

изучения:

- первоисточников,
- дат и событий,
- терминологии.

ответов:

- на вопросы для самопроверки,

подготовки:

- сообщений,
- рефератов,
- презентаций.

решений:

- заданий,
- тестов.

6.1. Задания для приобретения, закрепления и углубления знаний.

6.1.1 Основные категории учебной дисциплины для самостоятельного изучения:

Информация – это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством для нужд человека. Информация необходима каждому как условие и как средство существования человека в обществе. И поэтому так же нуждается в защите, как среда обитания, пища и все остальные элементы жизнедеятельности.

Информационно-психологическую безопасность в общем виде можно определить как состояние защищенности индивидуальной, групповой и общественной психологии социальных субъектов различных уровней общности от разрушительного воздействия на сознание негативных информационных факторов.

Применительно к конкретному человеку информационно-психологическая безопасность – это состояние защищенности сознания и психического здоровья человека, обеспечивающее его целостность как социального субъекта, возможность адекватного поведения и личностного развития в условиях неблагоприятных информационных воздействий.

Информационное противоборство – это комплексное взаимное информационное воздействие сторон друг на друга, которое способно привести к принятию благоприятных для инициатора воздействия решений либо парализовать информационную инфраструктуру противника. Методы воздействия: радиоэлектронная борьба, компьютерные конфликты, действия на психологическом и мировоззренческом уровнях, вброс ложной или компрометирующей информации, внушение, навязывание и т. п.

Более острая стадия противоборства – информационная война – согласованная деятельность по использованию информации как оружия для разрушающего воздействия на противника в различных сферах: экономической, политической, социальной и на поле боя. Информационная война – война нового типа, ее основным объектом являются не только информационные системы, но, прежде всего, сознание людей, их поведение и здоровье.

Информационная угроза – опасность, содержание которой составляют различная информация или ее комбинации, которые могут быть использованы против социального или социально-технического объекта (системы) с целью изменения его интересов, потребностей, ориентаций в соответствии с целями субъекта информации.

Информационный риск – вероятность информационной угрозы и реальных действий противника, мера измерения успешности или опасности возможных воздействий. Риск зависит от характера воздействий и объекта воздействий, от условий их осуществления, а также от возможностей защиты.

Компьютерные вирусы – программные средства, способные размножаться, прикрепляться к программам, передаваться по линиям связи и сетям передачи данных, проникать в электронные телефонные станции и системы управления и выводить их из строя.

«Логические бомбы» – такое название получили программные закладные устройства, заранее внедряемые в информационно-управляющие центры военной и гражданской инфраструктуры, которые по сигналу или в установленное время приводятся в действие, уничтожая или искажая информацию и дезорганизуя работу программно-технических средств.

Известны два вида указанных антивирусных средств:

- программы-фильтры,
- аппаратные средства контроля.

Программы-фильтры, называемые также резидентными сторожами и мониторами, постоянно находятся в оперативной памяти и перехватывают заданные прерывания с целью контроля подозрительных действий.

Встроенные аппаратные средства ПК обеспечивают контроль модификации системного загрузчика и таблицы разделов жесткого диска, находящихся в главной загрузочной записи диска (MBR). Включение указанных возможностей в ПК осуществляется с помощью программы Setup, расположенной в ПЗУ. Следует указать, что

программу Setup можно обойти в случае замены загрузочных секторов путем непосредственного обращения к портам ввода-вывода контроллеров жесткого и гибкого дисков.

Криптография – наука о шифрах.

Шифрование (зашифрование) – процесс применения шифра к защищаемой информации, т. е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре.

Дешифрование – процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

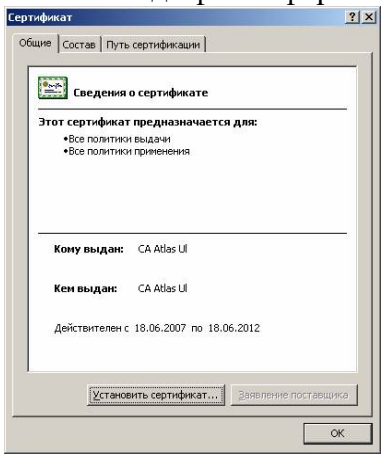
Криптография – прикладная наука, она использует самые последние достижения фундаментальных наук, в первую очередь, математики. С другой стороны, все конкретные задачи криптографии существенно зависят от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации.

Под ключом в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения.

Криптография – наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

Криптоанализ – наука (и практика ее применения) о методах и способах вскрытия шифров.

Фактически, ЭЦП представляет собой совокупность закрытого ключа - контейнера, обладателем которого может быть только владелец сертификата, и однозначно соответствующего этому закрытому ключу открытого ключа – сертификата. Сертификат представим в виде файла формата X.509 (см. рис).



Аутентификацией (установлением подлинности) называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется идентификацией.

Геометрия руки. Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2 %.

· Радужная оболочка глаза. Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из 1078.

· Термический образ лица. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных сотрудников и отсеивания

посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок.

· Голос. Проверка голоса удобна для использования в телекоммуникационных приложениях. Необходимые для этого 16-разрядная звуковая плата и конденсаторный микрофон стоят менее 25 $. Вероятность ошибки составляет 2 – 5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления идентификации личности и его состояния по голосу – возбужден, болен, говорит правду, не в себе и т.д.

· Ввод с клавиатуры. Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями.

· Подпись. Для контроля рукописной подписи используются дигитайзеры.

После выполнения идентификации и аутентификации необходимо установить полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования вычислительных ресурсов, доступных в АС. Такой процесс называется разграничением (логическим управлением) доступа.

Регистрация представляет собой механизм подотчетности системы ОБИ, фиксирующий все события, касающиеся безопасности, такие как: вход и выход субъектов доступа, запуск и завершение программ, выдача печатных документов, попытки доступа к защищаемым ресурсам, изменение полномочий субъектов доступа и статуса объектов доступа и т. д.

Аудит – анализ протоколируемой информации.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Принцип безопасности – затраты на средства защиты не должны превышать стоимости защищаемых объектов.

Использование АС связано с определенной совокупностью рисков, под которыми понимаются стоимостные выражения событий (обычно вероятностных), ведущих к потерям.

Под угрозой обычно понимают любое событие (действие), которое потенциально может нанести ущерб АС путем нарушения конфиденциальности, целостности или доступности информации.

План защиты – документ, определяющий текущую реализацию системы ОБИ и необходимый в повседневной работе.

К основным процедурам обеспечения безопасности относятся:

- проверка системы и средств безопасности; управление паролями; управление счетами; поддержка пользователей; сопровождение программного обеспечения; конфигурационное управление; резервное копирование; управление носителями; документирование.

Первая обязанность администратора – это эксплуатация и научно-техническое сопровождение вверенного ему программного обеспечения.

В связи с этим, администратор должен выполнять следующие действия:

- контролировать безопасность вычислительного процесса с целью выявления компьютерных вирусов, сбоев и отказов функционирования программ и запуска неавторизованных программ и процессов;

- контролировать целостность программного обеспечения (неавторизованную модификацию) на предмет выявления программных закладок, недокументированных функций и других программных дефектов;

- обеспечивать восстановление программ с эталонных копий (возможно, с привлечением сил и средств фонда алгоритмов и программ предприятия), их обновление, замену и другие вопросы, касающиеся жизненного цикла программного обеспечения.

6.2 Задания для повторения и углубления приобретаемых знаний.

Задание 6.2.1. З1(ПК-1) *Информация и необходимость ее защиты.*

1. Аргументируйте необходимость защиты информации.
2. Что такое массовая и конфиденциальная информация?
3. Какие бывают виды тайн?

Задание 6.2.2. З2(ПК-1) *Информация и необходимость ее защиты.*

1. Охарактеризуйте информацию как объект права собственности.
2. Охарактеризуйте информационную безопасность как составляющую национальной безопасности страны.
3. Охарактеризуйте основные законодательные акты и нормативные документы, касающиеся государственной тайны и защиты информации в России.

Задание 6.2.3 З3(ПК-1) *Угрозы информационной безопасности.*

1.Охарактеризуйте классификацию и общий анализ угроз информационной безопасности. 2. Какие бывают виды возможных нарушений информационных систем?

3.охарактеризуйте случайные угрозы информационной безопасности.

4. Перечислите преднамеренные угрозы информационной безопасности.

Задание 6.2.4 З4(ПК-1) *Угрозы информационной безопасности.*

1. Каковы основные пути распространения компьютерных вирусов?
2. Назовите уровни и средства антивирусной защиты.
3. Методы защиты от известных вирусов?
4. Методы защиты от неизвестных вирусов?
5. Что понимается под термином «сканер» в системе с антивирусной защитой?
6. Принципы защиты от проявления вирусов?
7. Дайте оценку антивирусного средства, установленного на Вашем личном компьютере.
8. Что понимается под проактивной защитой от вирусов?

6.3. Задания, направленные на формирование профессиональных умений.

Задание 6.3.1. У1(ПК-1)

Составьте презентацию «Роль и место информационной безопасности».

Задание 6.3.2. У2(ПК-1)

Подготовьте реферат на тему «Государственная тайна и защита информации в России».

Задание 6.3.3. У3(ПК-1)

Подготовьте эссе на тему «Угрозы информационной безопасности в социально-экономических системах».

Задание 6.3.4. У4(ПК-1)

Составьте презентацию «Средства антивирусной защиты».

6.4. Задания, направленные на формирование профессиональных навыков, владений

Задание 6.4.1. В1(ПК-1)

Изучить и получить навык применения программно-технических средств контроля выполнения требований политики безопасности организации.

Используя полученные знания, спланировать и описать области проверки в рамках аудита информационной безопасности вымышленной компании.

Получения навыков в создании итоговой документации по результатам проведенного аудита.

Ознакомление с представленными средства инструментального контроля

Изучение возможностей представленных средств контроля.

Проведение пробных проверок систем/компьютеров установленных в учебном классе.

Получение одного либо нескольких отчётов и подготовка предложений по устранению выявленных несоответствий.

Подготовка плана мероприятий по аудиту информационной безопасности

Формулирование требований аудита на основании одного из стандартов информационной безопасности.

Разработка плана мероприятий с указанием сроков, подразделений и видов проверок для выбранной компании.

Разработка итогового отчёта по результатам аудита.

Подготовка простейшей методики анализа результатов аудита.

Подготовка формы аудиторского отчёта с указанием персонала, его заполняющего, и плана проведения повторных проверок.

Задание 6.4.2. В2(ПК-1)

Откройте два терминала (в серверных Linux для переключения между терминалами (tty) обычно используется сочетание клавиш Alt+F[1-5]). В одном из них получите права суперпользователя используя команду sudo su:

Изучите как создать пользователя с домашним каталогом с помощью команды useradd из справочной документации man

Используя useradd создайте пользователя «sit2» с домашним каталогом «sit2».

Установите пароль для нового пользователя «sit2» с помощью команды passwd sit2

Выйдите из суперпользователя командой exit

Войдите под первым терминалом в пользователя «sit», во втором в пользователя «sit2».

Посмотрите какой идентификатор получил пользователь «sit» и пользователь «sit2» используя команду id

Посмотрите права доступа на домашний каталог пользователей «sit» и «sit2», используя команду ls

Создайте файл под пользователем «sit2» с маской 0077 используя umask

Попробуйте прочитать его содержимое под пользователем «sit» используя команду cat

Задание 6.4.3. В3(ПК-1)

Измените права доступа на файл так, чтобы пользователь «sit» мог записывать в файл, но не читать его.

Запишите текстовую информацию в файл из под пользователя «sit» используя консольный текстовый редактор vi или nano

Проверьте права на файл, и прочитайте его содержимое из под пользователя «sit2»

Создайте каталог из под пользователя «sit2»

Установите права записи для группы пользователей на данный каталог

Добавьте пользователя «sit» в группу «sit2» с помощью команды usermod

Проверьте в какие группы входит пользователь «sit»

Создайте несколько файлов в каталоге, который был создан пользователем «sit2» из под пользователя «sit».

Ознакомьтесь как удалить пользователя вместе с содержимым его домашнего каталога из справочной документации

Удалите пользователя «sit2» вместе с его домашним каталогом.

Задание 6.4.4. В4(ПК-1)

Добавьте в виртуальную машину с операционной системой Linux виртуальный

жесткий диск (делается это в настройках виртуальной машины).

Запустите виртуальную машину с операционной системой Linux.

Ознакомьтесь с командой fdisk и ее возможностями из справочной документации.

Создайте таблицу разделов (3 первичных и 1 логический) с помощью команды fdisk на добавленном виртуальном диске (обычно это диск /dev/sdb).

Запишите изменения на диск

Проверьте факт создания разделов используя команду fdisk. (Так же, создание разделов можно проверить используя команду ls /dev/sd*)

Отформатируйте созданные разделы в файловую систему ext4.

Ознакомьтесь с командами mount и umount и их возможностями из справочной документации.

Смонтируйте созданные разделы и создайте там произвольные файлы.

Сделайте резервную копию MBR с помощью утилиты DD.

Сотрите таблицу разделов MBR с помощью утилиты DD.

Восстановите MBR с помощью утилиты DD.

Смонтируйте разделы и проверьте целостность данных.

Отмонтируйте разделы.

Соотношение заданий с формируемыми показателями обучения

Формируемая компетенция	***Показатели сформированности компетенции***	***Задания, направленные на: - приобретение новых знаний, углубления и закрепления ранее приобретенных знаний; - формирование профессиональных умений и навыков***
ПК-1 Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.	**Владеть:** - способностью формировать требования к информационной системе в процессе обследования организации и выявления информационной потребности пользователей В1(ПК-1); - методами проектирования информационных систем, стадии и этапы процесса проектирования с учетом выявленных информационных потребностей пользователей обследованной организации В2(ПК-1); - технологией осуществлять содержательное описание бизнес-процесса организации в терминах предметной области с учетом социально-культурных явлений и процессов В3(ПК-1); - навыками постановки целей и задач имитационного моделирования бизнес-процессов организации В4(ПК-1).	**Задание 6.4.5** В1(ПК-1) **Задание 6.4.6** В2(ПК-1) **Задание 6.4.7** В3(ПК-1) **Задание 6.4.8** В4(ПК-1)
	Уметь: - проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе У1(ПК-1); - собирать и систематизировать информацию о структуре организации и ее бизнес-процессах в рамках информационной безопасности и безопасности жизнедеятельности пользователей организации У2(ПК-1); - осуществлять содержательное описание бизнес-процесса организации в терминах предметной области с учетом социально-культурных явлений и процессов У3(ПК-1); - выявлять внешние и внутренние случайные	**Задание 6.3.5.** У1(ПК-1) **Задание 6.3.6.** У2(ПК-1) **Задание 6.3.7.** У3(ПК-1) **Задание 6.3.8.** У4(ПК-1)

	факторы, влияющие на бизнес-процессы предприятия с целью раскрытия информационных потребностей пользователей и формирования требования к информационной системе организации У4(ПК-1).	
	Знать: - виды и формы процесса обследования организаций, выявления информационных потребностей пользователей и формирование требований к информационной системе З1(ПК-1); - основные понятия информационного менеджмента, маркетинга, теории систем и системного анализа, теории экономических, предметно-ориентированных, корпоративных, интеллектуальных информационных систем, систем электронной коммерции, информационной безопасности в рамках обследования организации З2(ПК-1); - принципы проектирования информационных систем, стадии и этапы процесса проектирования с учетом выявленных информационных потребностей пользователей обследованной организации З3(ПК-1); - сущность методологии имитационного моделирования бизнес-процессов сложных систем с учетом выявленных информационных потребностей пользователей обследованной организации З4(ПК-1).	**Задание 6.2.5** З1(ПК-1) **Задание 6.2.6** З2(ПК-1) **Задание 6.2.7** З3(ПК-1) **Задание 6.2.8** З4(ПК-1)

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Средства оценивания в ходе текущего контроля:

7.1.1 Задания для оценки знаний

7.1.1.1 Тестовые задания (ПК-1)

Вопрос № 1: Какой метод поиска КВ предполагает, что антивирусные программы должны постоянно находиться в оперативной памяти компьютера и отслеживать все подозрительные действия, выполняемые другими программами?

1. Метод резидентных сторожей

2. Метод эвристического анализа

3. Вакцинирование

4. Метод обнаружения изменений

Вопрос № 2: Какой из методов поиска КВ заключается в том, что антивирусная программа предварительно запоминает характеристики всех областей диска, которые могут подвергаться нападению КВ, а затем периодически проверяет их?

1. Метод обнаружения изменений

2.Метод сканирования

3. Метод эвристического анализа

4. Вакцинирование

Вопрос № 3: В какой стране разработан персональный идентификатор eToken?

1. Израиль

2. США

3. Германия

4. Россия

Вопрос № 4: Какие цели преследует защита программного обеспечения?

1.ограничение несанкционированного доступа к программам или их преднамеренное разрушение и хищение

2. исключение несанкционированного копирования (тиражирования) программ

3. обеспечение физической охраны средств вычислительной техники

4. обучение персонала новым методам работы

Вопрос № 5: Какие две категории из перечисленных относятся к категориям авторского права?

1.экономические права, дающие их обладателям право на получение экономических выгод от продажи или использования программных продуктов и баз данных

2. моральные права, обеспечивающие защиту личности автора в его произведении

3. человеческие права, дающие право человеку чувствовать гордость за созданный им программный продукт

4. дружеские права, дающие возможность друзьям автора распространять и использовать его программные продукты и базы данных

Вопрос № 6: Как выглядит знак авторского права?

1. ©

2. ®

3. TM

4. WWW

Вопрос № 7: Какой вид лицензии предполагает продажу всех имущественных прав на программный продукт или базу данных, покупателю лицензии предоставляется исключительное право на их использование, а автор или владелец патента отказывается от самостоятельного их применения или предоставления другим лицам?

1.Исключительная лицензия

2. Простая лицензия

3. Этикеточная лицензия

4. Коробочная лицензия

Вопрос № 8: Какой вид лицензии распространяется на одну копию программного продукта или базы данных?

1.Одиночная лицензия

2. Исключительная лицензия

3. Простая лицензия

4. Этикеточная лицензия

Вопрос № 9: Какая лицензия предоставляет право лицензиату использовать программный продукт или базу данных, оставляя за собой право применять их и предоставлять на аналогичных условиях неограниченному числу лиц (лицензиат при этом не может сам выдавать сублицензии, может лишь продать копии приобретенного программного продукта или базы данных)?

1. Простая лицензия

2. Этикеточная лицензия

3. Исключительная лицензия

4. Неполная лицензия

Вопрос № 10: Какой вид лицензии приобретают дилер (торговец) либо фирмы-производители, использующие купленные лицензии как сопутствующий товар к основному виду деятельности?

1.Простая лицензия

2. Дополнительная лицензия

3. Суперлицензия

4. Магазинная лицензия

Вопрос № 11: Основными функции электронного архива являются:

1. Регистрация документов в системе (заполнение регистрационной карточки), присоединение к карточке любого количества файлов произвольного формата

2. Поиск документов по любому из полей регистрационной карточки и по тексту присоединенных к карточке файлов с учетом морфологии русского языка

3. Предупреждение персонала о приходе начальника

4. Пожарная сигнализация

Вопрос № 12: В результате внедрения системы электронного документооборота удается достичь:

1. повышения оперативности получения необходимой информации

2. увеличения затрат на хранение бумажных документов

3. повышения заработной платы бухгалтеров

4. отказа от использования SQL-технологии

Вопрос № 13: Как расшифровывается аббревиатура ФСТЭК России?

1.Федеральная служба по экспортному и техническому контролю

2. Федеральная специальная техническая комиссия экспертов

3. Федеральный совет технических экспертов криминалистов

4. Федеральная служба технико-экологического контроля

Вопрос №14: В каком случае ФСТЭК России не осуществляет функциональное регулирование деятельности по обеспечению защиты информации?

1.В случае если применяются криптографические методы защиты информации

2.В случае если не применяются криптографические методы защиты информации

3.В любом случае

4.Никогда не является

Вопрос № 15: Какой орган исполнительной власти осуществляет экспортный контроль?

1. ФСТЭК России

2. ФСБ России

3. МВД России

4. МИД России

Вопрос № 16: В задачи какого органа исполнительной власти входит осуществление государственной научно-технической политики в области защиты информации?

1. ФНС России

2. МВД России

3. Прокуратура РФ

4. ФСТЭК России

Вопрос № 17: Что не является задачей ФСТЭК России?

1. Реализация государственной политики и организация межведомственного взаимодействия в области экспортного контроля

2. Прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации

3. Организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а так же руководство указанной государственной системой

4. Разработка алгоритмов шифрования

Вопрос № 18: ФСТЭК России в целях реализации своих полномочий имеет право:

1. осуществлять радиоконтроль

2. издавать в пределах своей компетенции нормативные правовые акты, методические документы и индивидуальные правовые акты

3. утверждать квалификационные требования к специалистам, работающим в области агентурной разведки

4. приостанавливать или отменять действия выданных сертификатов

Вопрос № 19: При каком органе исполнительной власти действует Академия криптографии России?

1.ФСБ России
2. МинФине России
3. ФСТЭК России
4. МО России

Вопрос № 20: В задачи какого органа исполнительной власти входит осуществление государственной научно-технической политики в области обеспечения информационной безопасности?

1.ФСБ России
2. ФСТЭК России
3. МО России
4. ФНС России

Вопрос № 21: Что не является функцией ФСБ России?

1. участие в разработке и реализации мер по обеспечению информационной безопасности страны и защите сведений, составляющих государственную тайну
2. осуществляет и организует в соответствии с федеральным законодательством лицензирование отдельных видов деятельности
3. занимается сертификацией средств защиты информации от несанкционированного доступа
4. организует работу комиссий по аттестации автоматизированных систем по требованиям безопасности

Вопрос № 22: Какие два основных документа содержат совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации?

1. Доктрина информационной безопасности Российской Федерации
2. Концепция национальной безопасности Российской Федерации
3. Конвенция о защите информации Российской Федерации
4. Трактат о защите информации Российской Федерации

Вопрос № 23: К принципам построения системы защиты относятся:

1.Принцип системности
2.Принцип компетентности
3. Принцип разумной достаточности
4. Принцип неуправляемости

Вопрос № 24: Как называется программа (некоторая совокупность выполняемого кода/инструкций), которая способна создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д. без ведома пользователя (при этом копии сохраняют способность дальнейшего распространения)?

1. Компьютерный вирус
2. Прикладное ПО
3. Компьютерный помощник
4. Плохая программка

Вопрос № 25: Какие два способа заражения среды обитания используют компьютерные вирусы?

1. Резидентный
2. Нерезидентный
3. Полурезидентный
4. Сетевой

Вопрос № 26: По особенностям алгоритма вирусы делятся на:

1.компаньон-вирусы (companion)
2. вирусы-“черви” (worm)
3. “полиморфик”-вирусы
4. касперский

Вопрос № 27: Как называются вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов?

1.паразитические
2. студенческие
3. "стелс"-вирусы
4. макро-вирусы

Вопрос № 28: Как называются вирусы, которые проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии?

1."полиморфик"-вирусы
2. "макро-вирусы"
3. "паразитические"
4. компаньон-вирусы (compаnion)

Вопрос № 29: Как называются действия третьей стороны, цель которых - подтвердить то, что изделие или услуга соответствует определенным стандартам или другим нормативным документам?

1.Сертификация
2. Лицензирование
3. Аттестация
4. Пробы

Вопрос № 30: Какой метод позволяет обнаруживать ранее неизвестные КВ, даже если они не пытаются изменять сектора и файлы?

1. Эвристический анализ
2. Резидентный сторож
3. Метод вакцинирования
4. Метод обнаружения изменений

№	***Показатели сформированности компетенции***	***ФОС текущего контроля (тестовые задания)***
1.	З1(ПК-1).	1-12,24-30
2.	З2(ПК-1).	1-30
3.	З3(ПК-1).	1-30
4.	З4(ПК-1).	1-30

7.1.2 Задания для оценки умений

7.1.2.1 Примерные темы сообщений (ПК-1)

Сообщения (устная форма) позволяет глубже ознакомиться с отдельными, наиболее важными и интересными процессами, осмыслить, увидеть их сложность и особенности.

1. Информация как объект права собственности.
2. Основные законодательные акты и нормативные документы, касающиеся информационной безопасности в России.
3. Российское законодательство в области охраны авторских прав.
4. Виды тайн.
5. Информационные войны.
6. Классификации угроз информационной безопасности.
7. Случайные угрозы информационной безопасности.
8. Внешние угрозы информационной безопасности.
9. Внутренние (инсайдерские) угрозы информационной безопасности.
10. Физическая защита информационных систем.
11. Программно-технические методы обеспечения информационной безопасности.
12. Регистрация и контроль действий пользователей
13. Криптографические методы защиты информации.

14. Шифрование.
15. Основные методы шифрования.
16. Стандарты шифрования.
17. Вредоносные программы.
18. Информационная безопасность в Интернете.
19. Стратегия злоумышленника при несанкционированном доступе.
20. Электронная цифровая подпись.
21. Критерии оценки безопасности компьютерных систем Министерства обороны США.
22. Европейские критерии безопасности информационных технологий.
23. Функционирование КСЗИ
24. Создание организационной структуры КСЗИ
25. Принципы построения КСЗИ

№	*Показатели сформированности компетенции*	*ФОС текущего контроля (тематика сообщений)*
1.	У1(ПК-1)	1-30
2.	У2(ПК-1)	1-30
3.	У3(ПК-1)	1-30
4.	У4(ПК-1)	1-30

7.1.2.2 Темы рефератов (ПК-1)

№	Тема	Опорные слова для раскрытия темы
1.	Информация как объект права собственности	Понятие информации. Свойство физической неотчуждаемости. Свойство обособляемости информации. Свойство информационной вещи. Свойство тиражируемости. Свойство организационной формы. Право распоряжения, право владения, право пользования. Информационный ресурс. Открытая информация. Документированная информации с ограниченным доступом. Цели защиты информации.
2.	Основные законодательные акты и нормативные документы, касающиеся информационной безопасности в России	Система информационного законодательства. Федеральные законы. Нормативные акты Президента РФ, Правительства РФ, ведомственные нормативные акты. ФЗ "Об информации, информационных технологиях и о защите информации". ГК РФ. УК РФ. ФЗ "О персональных данных". ФЗ " Об электронной подписи". ФЗ «О государственной тайне». ФЗ "О коммерческой тайне".
3.	Российское законодательство в области охраны авторских прав.	Конституция РФ. Четвертая часть Гражданского кодекса Российской Федерации. Международные акты в области авторского права. Объекты авторского права по законодательству РФ. Особенности производных и составных произведений. Программы для ЭВМ и базы данных как объект авторского права. Смежные права. Объекты интеллектуальной собственности, не являющихся объектами авторского права. Субъекты авторского права. Нарушения авторского права и его защита в РФ.
4.	Виды тайн.	Понятия тайны. Тайна частной жизни. Профессиональная тайна. Коммерческая тайна. Служебная тайна. Государственная тайна.
5.	Информационные войны.	Понятие информационной войны. История информационных войн. Холодная война. Основные черты информационной войны. Методы ведения информационных войн. Современные информационные войны.
6.	Классификации угроз информационной безопасности.	Классификация угроз по аспекту информационной безопасности. Природа возникновения угроз. Преднамеренность проявления угроз. Классификация угроз по способу осуществления. Классификация по расположению источника угроз. Классификация по способу доступа к ресурсам.
7.	Случайные угрозы информационной безопасности.	Понятия сбоя и отказа. Сбои и отказы в работе технических средств. Ошибки при разработке компьютерных систем. Ошибки обслуживающего персонала и пользователей. Техногенные происшествия и аварии. Случайные угрозы природного характера.

8.	Внешние угрозы информационной безопасности.	Компьютерные вирусы и вредоносные программы. Организации и отдельные лица как источники угроз. Стихийные бедствия. Формы проявления внешних угроз. Промышленный шпионаж. Комплексный подход к защите от внешних угроз.
9.	Внутренние (инсайдерские) угрозы информационной безопасности.	Источники внутренних угроз. Формы проявления внутренних угроз. Модель нарушителя. Технологии защиты от внутренних угроз. Контроль документов. Защита от утечек.
10.	Физическая защита информационных систем.	Задачи физических систем защиты информации. Средства предупреждения. Средства обнаружения. Системы ликвидации угроз. Классификация средств защиты по физической природе и функциональному назначению. Средства физической защиты. Системы контроля доступа
11.	Программно-технические методы обеспечения информационной безопасности.	Средства защиты от несанкционированного доступа (НСД). Системы анализа и моделирования информационных потоков (CASE-системы). Системы мониторинга сетей. Анализаторы протоколов. Антивирусные средства. Межсетевые экраны. Криптографические средства. Системы резервного копирования. Системы бесперебойного питания. Системы аутентификации. Средства предотвращения взлома корпусов и краж оборудования. Средства контроля доступа в помещения. Инструментальные средства анализа систем защиты.
12.	Регистрация и контроль действий пользователей	Идентификация и аутентификация. Регистрация пользователя в системе. Регистрация и учет событий в системе (аудит). Регистрационные журналы. Подсистема сигнализации.
13.	Криптографические методы защиты информации.	Криптография. Принципы криптографии. Кодирование. Сжатие. Шифрование. Типы шифров. Алгоритм RSA. Электронная подпись. ХЭШ-функция. Стеганография. Сертификация и стандартизация криптосистем. Шифрованные архивы.
14.	Шифрование.	Процесс шифрования. Алгоритм преобразования и ключ. Методы шифрования. Шифр. Атака на шифр (криптоанализ, криптоатака). Требования к методам шифрования. Криптостойкость шифра. Симметричное шифрование и его проблемы. Асимметричное шифрование. Метод открытого ключа. Алгоритмы RSA и DSA. Сертификаты открытых ключей. Центры сертификации.
15.	Вредоносные программы.	Понятие вредоносной программы. Вирусы и их виды. Жизненный цикл вируса. Троянские программы. Черви. Руткит. Утилиты скрытого управления. Загрузчики. Клавиатурные шпионы. Похитители паролей. Утилиты дозвона. Модификаторы настроек браузера. Спам- и DDOS-сервера. Логические бомбы. Условно опасные программы. Хакерские утилиты. Программы-шутки.
16.	Информационная безопасность в Интернете.	Рассылки спама. Использование компьютера пользователя для атак на другие компьютеры. Кража секретной информации. Мошенничество в Интернете. Фишинг. Компьютерные вирусы и вредоносные программы. Правила безопасности при работе в сети Интернет. Безопасность в социальных сетях. Безопасность платежей в Интернете. Безопасность покупок в интернете. Безопасность детей в Интернете. «Группы смерти». Правила поведения на форумах.
17.	Стратегия злоумышленника при несанкционированном доступе.	Инициативное сотрудничество. Склонение к сотрудничеству, вербовка. Выпытывание. Подслушивание. Негласное осведомление. Наблюдение. Хищение. Копирование информации. Подделка (фальсификация) информации. Уничтожение информации. Незаконное подключение. Перехват. Фото- и видеосъемка. Сбор и аналитическая обработка информации, получаемой легальными и нелегальными путями.
18.	Электронная цифровая подпись.	Понятие электронной цифровой подписи и ее техническое обеспечение. Закрытый и открытый ключ. Электронный документ. Владелец сертификата ключа подписи. Удостоверяющий центр. Хеш-функция. Юридическая сила ЭЦП. Срок действия ЭЦП.
19.	Критерии оценки безопасности компьютерных систем Министерства обороны США.	TCSEC - "Оранжевая книга". Общая структура требований TCSEC. Политика безопасности. Подотчетность. Гарантии (корректность). Классы защищенности компьютерных систем по TCSEC. Интерпретация и развитие TCSEC.
20	Европейские критерии	Information Technology Security Evaluation Criteria (ITSEC). Основные

	безопасности информационных технологий.	понятия. Функциональные критерии. Критерии адекватности.

№	*Показатели сформированности компетенции*	*ФОС текущего контроля (тематика рефератов)*
1.	У1(ПК-1)	1-20
2.	У2(ПК-1)	1-20
3.	У3(ПК-1)	1-20
4.	У4(ПК-1)	1-20

7.1.2.3. Примерная тематика презентаций (ПК-1)

Презентация – набор слайдов в Power Point. Выступление по презентации не требуется и оценивается дополнительно.

Преподаватель каждый раз выбирает самостоятельно количество слайдов (в зависимости от количества учебных часов по дисциплине) от 10 слайдов и до 30 по одной проблематике.

Название документа – ФИО студента (Иванов И.П.ppt);

Первый слайд – тема презентации, далее – сам материал. План, актуальность темы, введение, заключение и список литературы не являются составной частью презентации и делаются студентом по собственному желанию.

Презентация в обязательном порядке включает следующие элементы:

- картинки и фото;
- графические элементы;
- классификации;
- таблицы;
- логические цепочки;
- схемы;
- выводы.

Ссылка при цитировании на источник в презентации обязательна. Все данные должны быть сопровождены годами.

1. Презентация на тему «Национальные интересы и безопасность»
   - Национальная безопасность
   - Основные объекты национальной безопасности
   - Составляющие национальной безопасности
   - Политическая, экономическая и военная безопасность.
   - Информационная безопасность
   - Национальные интересы
2. Презентация на тему «Национальные интересы и безопасность России»
   - Национальная безопасность РФ
   - Национальные интересы РФ
   - Основные сферы национальных интересов РФ
   - Приоритеты национальной безопасности РФ
   - Основные угрозы национальной безопасности РФ
   - Система обеспечения национальной безопасности РФ
3. Презентация на тему «Основные угрозы безопасности России»
   - Стратегия национальной безопасности РФ
   - Источники угроз военной безопасности Российской Федерации
   - Источники угроз национальной безопасности в сфере государственной и
   - общественной безопасности
   - Система обеспечения национальной безопасности
4. Презентация на тему «Информационная безопасность»
   - Понятие информационной безопасности

- Основные составляющие информационной безопасности
- Основные определения и критерии классификации угроз
- Объекты защиты
- Методы защиты
- Система информационной безопасности

5. Презентация на тему «Информационная война»
   - Понятие информационной войны
   - Черты информационной войны
   - Цели информационной войны
   - Методы ведения информационной войны
   - Методы и технологии защиты
6. Презентация на тему «Информационное оружие»
   - Понятие информационного оружия
   - Характерные черты информационного оружия
   - Виды информационного оружия
   - Защита от информационного оружия
7. Презентация на тему «Государственная система по обеспечению информационной безопасности»
   - Принципы национальной информационной безопасности
   - Основные задачи в сфере государственной информационной безопасности
   - Функции государственной системы по обеспечению информационной безопасности
8. Презентация на тему «Отечественные и зарубежные стандарты в области информационной безопасности»
   - Действующие ГОСТы в области информационной безопасности
   - Стандарт Министерства обороны США TSEC (Критерии Оценки Защищенности Надежных Систем) или «Оранжевая книга»
   - Инструкции Министерства обороны США NCSC-TG-005 и NCSC-TG-011 («Красная книга»)
   - Стандарт Агентства информационной безопасности ФРГ - Green Book («Зеленая книга»)
   - Европейский стандарт ITSEC (Критерии Оценки Защищенности Информационных Технологий) или «Белая книга»
9. Презентация на тему «Правовые основы защиты информации»
   - Федеральный закон № 149–ФЗ «Об информации, информационных технологиях и о защите информации»
   - Закон РФ «О государственной тайне»
   - Федеральный закон РФ № 161-ФЗ «О национальной платежной системе»
   - Федеральный закон РФ № 63-ФЗ «Об электронной подписи»
   - Федеральный закон РФ № 98-ФЗ «О коммерческой тайне»
   - Федеральный закон РФ № 152-ФЗ «О персональных данных»
   - Гражданский кодекс Российской Федерации № 230-ФЗ
   - Трудовой кодекс Российской Федерации № 197-ФЗ8
10. Презентация на тему «Ответственность за нарушение законодательства в информационной сфере»
    - Уголовная ответственность за нарушение законодательства в информационной сфере
    - Административная ответственность за нарушение законодательства в информационной сфере
    - Гражданско-правовая ответственность за правонарушения в информационной сфере
11. Презентация на тему «Защита информации в автоматизированных системах обработки

данных»
- Основные виды информации, подлежащие защите в АСОД
- Угрозы информации в АСОД
- Механизмы защиты
- Управление механизмами защиты

12. Презентация на тему «Каналы несанкционированного получения информации в АСОД (КНПИ)»
- Каналы, проявляющиеся безотносительно к обработке информации и без доступа злоумышленника к элементам ЭВТ
- Каналы, проявляющиеся в процессе обработки информации без доступа злоумышленника к элементам АСОД
- Каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АСОД, но без изменения последних
- Каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АСОД, но без изменения последних
- Каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам ЭВТ с изменением последних
- Каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к объектам ЭВТ с изменением элементов ЭВТ

13. Презентация на тему «Преднамеренные угрозы безопасности АСОД»
- Классификация угроз по цели реализации
- Классификация угроз по принципу воздействия на АСОД
- Классификация угроз по характеру воздействия на АСОД
- Классификация угроз по причине появления используемой ошибки защиты
- Классификация угроз по способу воздействия на АСОД
- Классификация угроз по объекту атаки
- Классификация угроз по используемым средствам атаки
- Классификация угроз по состоянию объекта атаки

14. Презентация на тему «Функции и задачи защиты информации»
- Методы формирования функций защиты
- Классы задач защиты информации
- Функции защиты
- Состояния и функции системы защиты информации

15. Презентация на тему «Методы парольной защиты»
- Пароль как метод аутентификации
- Использование простого пароля
- Использование динамически изменяющегося пароля
- Одноразовые пароли
- Организация парольной защиты

16. Презентация на тему «Своевременное обнаружение несанкционированных действий пользователей»
- Периодический контроль целостности информации;
- Регистрация действий пользователя
- Сигнализация о несанкционированных действиях пользователя
- Контроль правильности функционирования системы защиты

17. Презентация на тему «Криптографические методы защиты информации»
- Шифрование
- Стеганография
- Кодирование
- Сжатие

18. Презентация на тему «Комбинированные методы шифрования»
- Двойное шифрование

- Тройное шифрование с двумя ключами
- Тройное шифрование с тремя ключами
- Схема xDES1
- Пятикратное шифрование
- Отбеливание
- Каскадное применение блочных алгоритмов
- Объединение различных блочных алгоритмов

19. Презентация на тему «Защита информации в персональных компьютерах»
    - Особенности защиты информации в персональных компьютерах
    - Угрозы информации в персональных компьютерах
    - Обеспечение целостности информации в ПК
    - Защита от несанкционированного доступа
    - Разграничение доступа к элементам защищаемой информации
    - Защита информации от копирования
    - Защита компьютера от вредоносных закладок
20. Презентация на тему «Опознавание (аутентификация) пользователей и используемых компонентов обработки информации»
    - Распознавание по простому паролю
    - Опознавание в диалоговом режиме
    - Опознавание по индивидуальным особенностям и физиологическим характеристикам
    - Опознавание по радиокодовым устройствам
    - Опознавание по специальным идентификационным карточкам
    - Средства опознавания компонентов обработки данных
21. Презентация на тему «Защита информации от копирования»
    - Защита программы с использованием «нестандартного» носителя
    - Использование подхода SaaS
    - Отдельные средства защиты непосредственно кода приложения
    - Использование механизмов активации программного обеспечения
    - Программные системы защиты флеш-накопителя от копирования
    - Защита от несанкционированного доступа к компьютеру
22. Презентация на тему «Компьютерные вирусы и антивирусные программы»
    - Вредоносные программы
    - Особенности компьютерных вирусов
    - Классификация вирусов
    - Методы защиты от вирусов
    - Меры предотвращения заражения
    - Антивирусные программы

№	*Показатели сформированности компетенции*	*ФОС итогового контроля (тематика презентаций)*
1.	У1(ПК-1)	1-22
2.	У2(ПК-1)	1-22
3.	У3(ПК-1)	1-22
4.	У4(ПК-1)	1-22

7.1.3 Задания для оценки навыков, владений, опыта деятельности

7.2.3.1 Задачи по дисциплине (ПК-1)

Задача 1.

Разграничение прав доступа.

Откройте два терминала (в серверных Linux для переключения между терминалами (tty) обычно используется сочетание клавиш Alt+F[1-5]). В одном из них получите права

суперпользователя используя команду sudo su:

Изучите как создать пользователя с домашним каталогом с помощью команды useradd из справочной документации man

Используя useradd создайте пользователя «sit2» с домашним каталогом «sit2».

Установите пароль для нового пользователя «sit2» с помощью команды passwd sit2

Выйдите из суперпользователя командой exit

Войдите под первым терминалом в пользователя «sit», во втором в пользователя «sit2».

Посмотрите какой идентификатор получил пользователь «sit» и пользователь «sit2» используя команду id

Посмотрите права доступа на домашний каталог пользователей «sit» и «sit2», используя команду ls

Создайте файл под пользователем «sit2» с маской 0077 используя umask

Попробуйте прочитать его содержимое под пользователем «sit» используя команду cat

Измените права доступа на файл так, чтобы пользователь «sit» мог записывать в файл, но не читать его.

Запишите текстовую информацию в файл из под пользователя «sit» используя консольный текстовый редактор vi или nano

Проверьте права на файл, и прочитайте его содержимое из под пользователя «sit2»

Создайте каталог из под пользователя «sit2»

Установите права записи для группы пользователей на данный каталог

Добавьте пользователя «sit» в группу «sit2» с помощью команды usermod

Проверьте в какие группы входит пользователь «sit»

Создайте несколько файлов в каталоге, который был создан пользователем «sit2» из под пользователя «sit».

Ознакомьтесь как удалить пользователя вместе с содержимым его домашнего каталога из справочной документации

Удалите пользователя «sit2» вместе с его домашним каталогом.

Задача 2.

Шифрование данных.

Установить PGP, GPG <sudo apt-get install pgpgpg>

Произвести операции шифрования и дешифрования над произвольными файлами. Для шифрования используйте команду <gpg -c>. Для дешифрования <gpg –decrypt-file> (В этом случае в директории зашифрованного файла будет создан расшифрованный. Если нужно лишь вывести на экран расшифрованное содержимое используйте <gpg –decrypt>)

Установить TrueCrypt. Нам потребуется версия 7.1a. Скачать её можно здесь или здесь.

Создать криптоконтейнер, примонтировать его как виртуальный диск.

Поместить в криптоконтейнер какую-то информацию.

Отмонтировать диск и переместить криптоконтейнер.

Повторно примонтировать криптоконтейнер как виртуальный диск. Убедиться, что крип-токонтейнер может передаваться и использоваться независимо.

Установить LUKS/dm-crypt <sudo apt-get update>, <sudo apt-get install cryptsetup>.

Создаем файл, где будем хранить зашифрованные данные. Самый простой способ <fallocate -l 512M /root/test1>, где /root - директория хранения файла, test1 - имя файла. Так же для создания этого файла можно использовать команду dd. <dd if=/dev/zero of=/root/test2 bs=1M count=512>. Третий способ - использовать команду dd и заполнить файл случайными данными. <dd if=/dev/urandom of=/root/test3 bs=1M count=512>.

Создать криптоконтейнер. <cryptsetup -y luksFormat /root/test1> (нужно будет согласиться переписать данные и задать пароль).

Открыть контейнер. <cryptsetup luksOpen /root/test1 volume1>. (volume1 - имя

контейнера, его мы задаем этой командой). При этом будет создан файл /dev/mapper/volume1.

Создать в нем файловую систему <mkfs.ext4 -j /dev/mapper/volume1>.

Создать папку для монтирования <mkdir /mnt/files>. Монтировать <mount /dev/mapper/volume1 /mnt/files>

Теперь перенесем какие_ниибудь файлы в криптоконтейнер. Например, скопируем папку /etc <cp -r /etc/* /mnt/files>.

Размонтировать <umount /mnt/files>.

Теперь закрываем volume1. <cryptsetup luksClose volume1>. После этого наши данные за-шифрованы.

Чтобы открыть их выполним <cryptsetup luksOpen /root/test1 volume1> и <mount /dev/mapper/volume1 /mnt/files>.

Задача 3.

Восстановление данных TestDisk

TestDisk — свободная программа для восстановления данных, предназначенная прежде всего для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора, после программных или человеческих ошибок (на-пример, потеря MBR).

Установка <sudo apt-get install testdisk>.

Запускаем TestDisk <sudo testdisk>.

Появляется окошко приветствия TestDisk, нам предлагается вести лог работы (для выпол-нения данной работы лог не требуется).

Выбираем нужный диск и нажимаем Enter.

Предлагается выбрать тип таблицы разделов, обычно TestDisk определяет все правильно, так что нажимаем Enter.

Выбираем Analise.

Выбираем QuickSearch.

Нам выводят таблицу разделов. Выбираем раздел и нажимаем P, чтобы вывести список файлов.

Выбираем файлы для восстановления и нажимаем C.

Выбираем папку, куда будут сохранены файлы и нажимаем C.

Восстановление данных PhotoRec

PhotoRec - это утилита, входящая в состав пакета TestDisk. Предназначена для восстанов-ления испорченных файлов с карт памяти цифровых фотоаппаратов (CompactFlash, Secure Digital, SmartMedia, Memory Stick, Microdrive, MMC), USB flash-дисков, жестких дисков и CD/DVD. Восстанавливает файлы большинства распространенных графических форма-тов, включая JPEG, аудио-файлы, включая MP3, файлы документов в форматах Microsoft Office, PDF и HTML, а также архивы, включая ZIP. Может работать с файловыми систе-мами ext2, ext3, ext4 FAT, NTFS и HFS+, причем способна восстановить графические файлы даже в том случае, когда файловая система повреждена или отформатирована.

Установка <sudo apt-get install testdisk>.

Запускаем PhotoRec <sudo photorec>.

Выбираем нужный диск и нажимаем Enter.

В нижнем меню можно выбрать File Opt, чтобы выбрать типы файлов для восстановления (по умолчанию выбраны все).

Чтобы начать восстановление нажмите Enter, выбрав Search.

У нас выбрана система ext4, поэтому выбираем первый вариант [ext2/ext3].

Если выбрать пункт FREE, то поиск будет произведен в пустом пространстве и в этом случае будут восстановлены только удаленные файлы, а если выбрать WHOLE, то поиск будет произведен на всем диске.

Теперь нужно указать директорию, куда будем сохранять нужные нам файлы.

Выбираем нужную папку и нажимаем C.

Выбираем файлы для восстановления и нажимаем C.

Восстановление данных Extundelete

xtundelete – утилита, позволяющая восстанавливать файлы, которые были удалены с раз-делов ext3/ext4.

Установка: <sudo apt-get install extundelete>.

Как только вы поняли, что удалили нужные файлы, необходимо отмонтировать раздел: <umount /dev/<partition> >

Зайдите в каталог, в который будут восстанавливаться удаленные данные. Он должен быть расположен на разделе отличном от того, на котором хранились восстанавливаемые данные: cd /<путь_к_каталогу_куда_восстанавливать_данные>

Запустите extundelete, указав раздел, с которого будет происходить восстановление и файл, который необходимо восстановить: sudo extundelete /dev/<partition> –restore-file /<путь к файлу>/<имя_файла>

Можно так же восстанавливать содержимое каталогов: sudo extundelete /dev/<partition> –restore-directory /<путь_к_директории>

Восстановление данных Foremost.

Foremost - консольная программа, позволяющая искать файлы на дисках или их образах по hex-данным, характерным заголовкам и окончаниям. Программа проверяет файлы на предмет совпадения заранее определённых hex-кодов (сигнатур), соответствующих наи-более распространённым форматам файлов. После чего экстрагирует их из диска/образа и складывает в каталог, вместе с подробным отчётом о том, чего, сколько и откуда было восстановлено. Типы файлов, которые foremost может сразу восстановить: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp. Есть возможность добавлять свои форматы (в конфигурационном файле /etc/foremost.conf), о которых про-грамма не знает.

Установка: <sudo apt-get install foremost>

Пример использования для восстановления изображений с диска /dev/sdb в каталог ~/out_dir: <sudo foremost -t jpg,gif,png,bmp -i /dev/sdb -o ~/out_dir>

Задания к практической работе

Добавьте в виртуальную машину виртуальный жесткий диск.

Запустите виртуальную машину с Linux.

Запустите fdisk (gdisk или parted) и создайте таблицу разделов MBR с разделами.

Отформатируйте созданные разделы в файловую систему ext4.

Установите TestDisk.

Удалите MBR (или таблицу разделов) с помощью команды DD.

Восстановите MBR (или таблицу разделов) с помощью TestDisk.

Смонтируйте восстановленные разделы и создайте там произвольные файлы.

Удалите созданные файлы.

С помощью TestDisk восстановите данные.

Создайте произвольный каталог и запишите туда данные каталога /var/log/ .

Удалите данные с созданного каталога.

С помощью PhotoRec восстановите данные.

Создайте произвольный каталог и запишите туда данные каталога /etc/ .

С помощью Extundelete или Foremost восстановите данные.

Задача 4.

Нагрузочное тестирование веб-сервера с Apache

Для тестирования используются 2 машины – одна с установленным и работающим Apache, вторая будет отсылать запросы и делать выводы о производительности web-сервера.

Тестирование на PHP-запросы:

Определить максимальное число параллельных запросов, при котором сервер нас не будет блокировать.

Провести тест при использовании максимального числа запросов.

Тестирование на HTML-запросы:

Определить максимальное число параллельных запросов

Провести тест при использовании максимального числа запросов.

Провести сравнение результатов и сформировать выводы.

Нагрузочное тестирование веб-сервера с Nginx.

Для тестирования используется 2 виртуальные машины – одна с установленным и рабо-тающим Nginx, которой будут отсылаться запросы, другая будет отсылать эти самые за-просы и делать выводы о производительности веб-сервера с Nginx.

Примечание

<sudo apt-get nginx> - Установка Nginx

Тестирование на PHP-запросы:

Определить максимальное число параллельных запросов, при котором сервер нас не будет блокировать.

Провести тест при использовании максимального числа запросов.

Сравнить с результатами, полученными при тестировании Apache

Тестирование на HTML-запросы:

Определить максимальное число параллельных запросов.

Провести тест при использовании максимального числа запросов.

Сравнить с результатами, полученными при тестировании Apache

Провести сравнение результатов и сформировать выводы.

Нагрузочное тестирование веб-серверов Apache с балансировщиком нагрузки.

Для тестирования используется 4 машины – две одинаковые с установленным и работаю-щим Apache в качестве веб-серверов, которые соединены с третьей машиной, которая вы-полняет роль балансировщика нагрузки, на нем работает Nginx, четвертая машина будет отсылать эти запросы серверу и делать выводы о производительности данной связки из балансировщика нагрузки на Nginx и двумя веб-серверами Apache.

Тестирование на PHP-запросы:

Провести тест при использовании максимального для Apache числа запросов

Провести тест при использовании максимального для Nginx числа запросов

Сравнить с предыдущими результатами и сформировать выводы

Тестирование на HTML-запросы:

Провести тест при использовании максимального для Apache числа запросов

Провести тест при использовании максимального для Nginx числа запросов

Сравнить с предыдущими результатами и сформировать выводы

Нагрузочное тестирование веб-серверов Nginx с балансировщиком нагрузки.

Для тестирования используется 4 виртуальные машины – две одинаковые с установлен-ным и работающим Nginx в качестве веб- серверов, которые соединены с третьей маши-ной, которая выполняет роль балансировщика нагрузки, на нем работает Nginx, четвертая машина будет отсылать эти запросы серверу и делать выводы о производительности дан-ной связки из балансировщика нагрузки на Nginx и двумя веб-серверами Nginx.

Тестирование на PHP-запросы:

Провести тест при использовании максимального для Apache числа запросов

Провести тест при использовании максимального для Nginx числа запросов

Сравнить с предыдущими результатами и сформировать выводы

Тестирование на HTML-запросы:

Провести тест при использовании максимального для Apache числа запросов

Провести тест при использовании максимального для Nginx числа запросов

Сравнить с предыдущими результатами и сформировать выводы.

№	*Показатели сформированности компетенции*	*ФОС итогового контроля (задачи по дисциплине)*
1.	В1(ПК-1)	1-4
2.	В2(ПК-1)	1-4
3.	В3(ПК-1)	1-4
4.	В4(ПК-1)	1-4

7.2 ФОС для промежуточной аттестации

7.2.1 Задания для оценки знаний

Вопросы к экзамену (ПК-1)

1. Понятие информационной безопасности. Информационная безопасность в современных условиях.
2. Необходимость и общественная потребность защиты информации.
3. Массовая и конфиденциальная информация.
4. Информационная безопасность как составляющая национальной безопасности.
5. Государственные органы РФ, обеспечивающие информационную безопасность.
6. Государственная тайна.
7. Коммерческая тайна.
8. Законодательные акты, касающиеся информационной безопасности в России.
9. Ответственность за правонарушения в информационной сфере.
10. Понятие угрозы. Виды угроз.
11. Случайные угрозы информационной безопасности.
12. Преднамеренные угрозы информационной безопасности.
13. Угроза хакерских атак.
14. Фишинговые атаки.
15. Спам. Защита от спама.
16. Информационная безопасность в сети Интернет.
17. Виды противников или «нарушителей».
18. Основные принципы обеспечения информационной безопасности в компьютерных системах.
19. Организационное обеспечение защиты информации.
20. Технические виды защиты информации.
21. Административные методы защиты информации.
22. Программные методы защиты информации.
23. Защита информации от случайных угроз.
24. Основные виды технических каналов утечки информации.
25. Противодействие наблюдению, подслушиванию.
26. Основные методы шифрования.
27. Стандарты шифрования.
28. Защита программных средств от несанкционированного копирования и исследования.
29. Защита от несанкционированного изменения структуры информационной систе-мы в процессе эксплуатации.
30. Методы и средства защиты от побочных электромагнитных излучений и наводок.
31. Вредоносные программы.
32. Компьютерные вирусы.
33. Антивирусное программное обеспечение.
34. Сетевые экраны.
35. Электронно-цифровая подпись.
36. Использование биометрических методов.

37. Криптографические средства защиты информации.
38. Технология открытых ключей.
39. Идентификация и аутентификация пользователей.
40. Разграничение прав доступа к компьютерным ресурсам.
41. Модели управления доступом к компьютерной системе.
42. Стандарты защищенности информации в компьютерных системах.
43. Критерии оценки безопасности компьютерных систем Министерства обороны США.
44. Документы Гостехкомиссии России по защите информации.
45. Европейские критерии безопасности информационных технологий.
46. Основные положения теории информационной безопасности информационных систем.
47. Модели безопасности и их применение.
48. Комплексная система защиты информации (КСЗИ).
49. Основные технологические этапы разработки КСЗИ.
50. Создание организационной структуры КСЗИ.

№	*Показатели сформированности компетенции*	*ФОС промежуточного контроля (вопросы к экзамену)*
1.	З1(ПК-1).	1-50
2.	З2(ПК-1).	1-50
3.	З3(ПК-1).	1-50
4.	З4(ПК-1).	42-50

7.2.2 Задания для оценки умений

В качестве фондов оценочных средств для оценки умений обучающегося используются задания, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.2)

7.2.3 Задания для оценки навыков, владений, опыта деятельности

В качестве фондов оценочных средств для оценки навыков, владений, опыта деятельности обучающегося используются задания, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.3).

8. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Литература

а) Основная

1. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

б) Дополнительная

1. Информационная безопасность: учебно-методич.комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.

2. Семененко В.А.Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)

3. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки

38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 c. — 978-5-4487-0299-0. — Режим доступа: http://www.iprbookshop.ru/77318.html

9. ПЕРЕЧЕНЬ КОМПЛЕКТОВ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО ПРИ ИЗУЧЕНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

При изучении учебной дисциплины (в том числе в интерактивной форме) предполагается применение современных информационных технологий. Комплект программного обеспечения для их использования включает в себя: операционная система Microsoft Windows 7 Pro, офисный пакет программ Microsoft Office Professional Plus 2010, офисный пакет программ Microsoft Office Professional Plus 2007, антивирусная программа Dr. Web Desktop Security Suite, архиватор 7-zip, аудиопроигрыватель AIMP, просмотр изображений FastStone Image Viewer, ПО для чтения файлов формата PDF Adobe Acrobat Reader, ПО для сканирования документов NAPS2, ПО для записи видео и проведения видеотрансляций OBS Studio, ПО для удалённого администрирования Aspia, правовой справочник Гарант Аэро, онлайн-версия КонсультантПлюс: Студент, электронно-библиотечная система IPRBooks, электронно-библиотечная система Юрайт, математические вычисления Mathcad 14 University, версия 1С для обучения программированию: 1С: Предприятие 8.2 Версия для обучения программированию

10. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. ЭБС IPRbooks (АйПиАрбукс) http://www.iprbookshop.ru
2. Библиотека электронных ресурсов исторического факультета МГУ. http://www.hist.msu.ru/ER/index.html -
3. Российская государственная публичная библиотека http://elibrary.rsl.ru/
4. Информационно-правовой портал «Гарант» www.garant.ru
5. Информационно-правовой портал «КонсультантПлюс» www.consultant.ru
6. Российская государственная публичная библиотека http://elibrary.rsl.ru/
7. Электронно-библиотечная система (ЭБС), Издательство Юстицинформ// http://e.lanbook.com/books/
8. Образовательная платформа ЮРАЙТ https://urait.ru
9. ЭБС IPRbooks (АйПиАрбукс) http://www.iprbookshop.ru

11. ОБУЧЕНИЕ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Изучение данной учебной дисциплины обучающимися с ограниченными возможностями здоровья осуществляется в соответствии с Приказом Министерства образования и науки РФ от 9 ноября 2015 г. № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн, «Положением о порядке обучения студентов – инвалидов и лиц с ограниченными возможностями здоровья», утвержденным приказом ректора от 6 ноября 2015 года №60/о, «Положением о службе инклюзивного образования и психологической помощи» АНО ВО «Российский новый университет» от 20 мая 2016 года № 187/о.

Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится преподавателями с учетом их индивидуальных психофизиологических особенностей и специфики приема передачи учебной информации.

С обучающимися по индивидуальному плану и индивидуальному графику проводятся индивидуальные занятия и консультации.

12. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации
Ауд. 403 (компьютерный класс № 4)
Специализированная мебель:
- столы студенческие;
- стулья студенческие;
- стол для преподавателя;
- стул для преподавателя;
- столы компьютерные;
- кресла компьютерные;
- шкаф для хранения раздаточного материала;
- доска (меловая);
- маркерная доска (переносная).
Технические средства обучения:
- проектор;
- ПК для преподавателя с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза;
- ПК для с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза;
- веб-камера;
- экран;
- колонки;
- микрофон.
Специализированное оборудование:
- наглядные пособия (плакаты)

Автор (составитель): ст. преп. Корнаухов А.Ю. _____
Подпись

год начала подготовки 2018

Аннотация рабочей программы учебной дисциплины ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Код и направление подготовки: **09.03.03 Прикладная информатика**
Направленность (профиль): **«Прикладная информатика в экономике»**

Цели дисциплины

Обеспечение профессионального образования, способствующего социальной, академической мобильности, востребованности на рынке труда, успешной карьере, сотрудничеству.

Формирование у обучающихся систематизированных профессионально значимых знаний по информационной безопасности и профессиональных умений и навыков, необходимых бакалавру прикладной информатики в экономике.

Изучение учебной дисциплины направлено на получение общих сведений о предмете информационная безопасность и умение применять основные совокупности методов информационной безопасности, позволяющие обеспечить защиту информации на всех уровнях в современных условиях.

Место дисциплины в структуре ОП бакалавриата.

Учебная дисциплина «Информационная безопасность» относится к вариативной части учебного плана (Б1.В.15).

Учебная дисциплина содержательно и логически связана с другими учебными дисциплинами, изучаемыми студентами:

-предшествует освоению данной дисциплины: Информатика и программирование, Вычислительные системы, сети и телекоммуникации, Проектирование информационных систем, Операционные системы, Программная инженерия, Базы данных, Управление информационными системами.

-после изучения данной дисциплины изучается: Предметно-ориентированные экономические и информационные системы, Системы электронной коммерции.

Требования к уровню освоения содержания курса:

В результате освоения дисциплины обучающийся должен овладеть следующими компетенциями:

ПК-1 - Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.

Содержание учебной дисциплины.

Тема 1.*Информация и необходимость ее защиты.*

Необходимость защиты информации. Массовая и конфиденциальная информация. Виды тайн. Информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности страны. Основные законодательные акты и нормативные документы, касающиеся государственной тайны и защиты информации в России.

Тема 2.*Угрозы информационной безопасности.*

Понятие угрозы информационной безопасности. Классификация и общий анализ угроз. Три вида возможных нарушений информационной системы. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности. Виды противников или «нарушителей». Понятия о видах вирусов. Реализация угроз.

Тема 3.*Защита информации.*

Защита информации от случайных угроз. Защита компьютерных систем от несанкционированного вмешательства. Криптографические методы защиты информации. Шифрование. Основные методы шифрования. Стандарты шифрования. Вредоносные программы. Компьютерные вирусы. Средства защиты от компьютерных вирусов. Профилактика заражения компьютерными вирусами. Анализ способов нарушений

информационной безопасности. Использование защищенных компьютерных систем.

Тема 4. *Стандарты в области защиты информации. Построение защищенных информационных систем.*

Международные стандарты информационного обмена. Стандарты защищенности информации в компьютерных системах. Критерии оценки безопасности компьютерных систем Министерства обороны США. Документы Гостехкомиссии России по защите информации. Европейские критерии безопасности информационных технологий. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Комплексная система защиты информации (КСЗИ). Основные технологии построения защищенных ЭИС.

Лист внесения изменений в рабочую программу учебной дисциплины «Информационная безопасность»

Рабочая программа рассмотрена и одобрена на 2020/2021 учебный год.
Протокол № 1 заседания кафедры ПЭ от «03» сентября 2020 г.

1. Актуализация перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины на 2020-2021 учебный год.

1.1.Пункт 8.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/ bcode/450371
2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449350

1.2.Пункт 8.2. Дополнительная литература

1. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 c. — 978-5-4487-0299-0. — Режим доступа: http://www.iprbookshop.ru/77318.html
2. Семененко В.А.Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)
3. Информационная безопасность: учебно-методич.комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.

Зав. кафедрой _____/Преснякова Д.В./

Лист внесения изменений в рабочую программу учебной дисциплины «Информационная безопасность»

Рабочая программа рассмотрена и одобрена на 2021/2022 учебный год.
Протокол № 10 заседания кафедры ПЭ от «11» июня 2021 г.

1. Актуализация перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины на 2021-2022 учебный год.

1.1.Пункт 8.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/ bcode/450371
2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449350

1.2.Пункт 8.2. Дополнительная литература

1. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 c. — 978-5-4487-0299-0. — Режим доступа: http://www.iprbookshop.ru/77318.html
2. Семененко В.А.Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)
3. Информационная безопасность: учебно-методич.комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.

Зав. кафедрой ____/Преснякова Д.В./