

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной и прикладной информатики

Дата подписания: 16.02.2023 14:54:03

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе

дисциплины «Организация и управление службой защиты информации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Организация и управление службой защиты информации на предприятии» является изучение структуры, логической организации и системы управления службой защиты информации как основного звена систем защиты информации.

Задачи изучения дисциплины

Основными обобщенными задачами дисциплины являются:

- определение места службы защиты информации в системе безопасности предприятия; объяснение функций службы защиты информации;
- обоснование оптимальной структуры и штатного состава службы защиты информации в зависимости от решаемых задач и выполняемых функций;
- установление организационных основ и принципов деятельности службы защиты информации;
- разрешение общих и специфических вопросов подбора, расстановки и обучения кадров, организации труда сотрудников службы защиты информации; раскрытие принципов, методов и технологии управления службой защиты информации.

Компетенции, формируемые в результате освоения дисциплины

Способен использовать основы правовых знаний в различных сферах деятельности (ОК-4);

Способен использовать нормативные правовые акты в профессиональной деятельности(ОПК-5);

Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

Разделы дисциплины

Структура службы информационной безопасности. Функции основных групп службы безопасности. Цели и задачи службы информационной безопасности. Организационные основы и принципы деятельности службы информационной безопасности. Лицензирование видов деятельности службы безопасности. Управление службой защиты информации. Организация информационно-аналитической работы. Организация работы с персоналом предприятия.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета

фундаментальной и прикладной

(наименование ф-та полностью)

информатики



Т.А. Ширабакина

(подпись, инициалы, фамилия)

«*01*» *02* 20*17* г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация и управление службой защиты информации

направление подготовки (специальность)

10.03.01

(шифр согласно ФГОС)

Информационная безопасность

и наименование направление подготовки (специальности)

Безопасность автоматизированных систем

наименование профиля, специализации или магистерской программы

форма обучения

очная

очная, очно-заочная, заочная

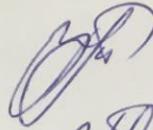
Курс – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования направления подготовки 10.03.01 – «Информационная безопасность» и на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Учёным советом университета, протокол «30» 01 2017г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 – «Информационная безопасность» на заседании кафедры информационной безопасности.

« 1 » февраля 2017г. Протокол № 9

Зав. кафедрой ИБ



Таныгин М.О.

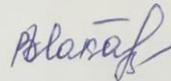
Разработчик программы
доцент кафедры ИБ



Таныгин М.О.

Согласовано:

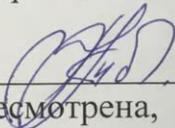
Директор научной библиотеки



Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № 05 «30» 01 2017г. на заседании кафедры информационной безопасности. Протокол № 7 «28» 08 2017г.

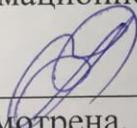
Зав. кафедрой



Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности. Протокол № 12 «29» 06 2017г.

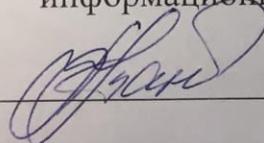
Зав. Кафедрой



Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности. Протокол № 11 «27» 06 2017г.

Зав. кафедрой



Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № 7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол № 1 от «31» 08 2020 г.

Зав. кафедрой _____



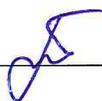
Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № 7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол № 11 от «28» 06 2021 г.

Зав. кафедрой _____



Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № 7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол № 11 от «30» 06 2022 г.

Зав. кафедрой _____



Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности. Протокол № от « » 20 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности. Протокол № от « » 20 г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Целью преподавания дисциплины «Организация и управление службой защиты информации» является изучение структуры, логической организации и системы управления службой защиты информации как основного звена систем защиты информации.

1.2. Задачи дисциплины

Основными обобщенными задачами дисциплины являются:

- определение места службы защиты информации в системе безопасности предприятия; объяснение функций службы защиты информации;
- обоснование оптимальной структуры и штатного состава службы защиты информации в зависимости от решаемых задач и выполняемых функций;
- установление организационных основ и принципов деятельности службы защиты информации;
- разрешение общих и специфических вопросов подбора, расстановки и обучения кадров, организации труда сотрудников службы защиты информации; раскрытие принципов, методов и технологии управления службой защиты информации

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать**:

- организацию судебных, правоприменительных и правоохранительных органов;
- правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности;
- основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права;
- основные нормативные правовые документы;
- информационные технологии в системе информационно-аналитического обеспечения безопасности;
- систему мер противодействия промышленному шпионажу;
- активные и пассивные методы сбора информации;
- составные части информационно-вычислительной сети-аппаратное и программное обеспечение, подлежащее защите;

уметь:

- использовать нормативно-правовые знания в различных сферах жизнедеятельности;
- ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу профессиональной деятельности;
- определять направления актуализации системы защиты информации в соответствии с текущими деловыми потребностями фирмы и выявленным уровнем уязвимости защищаемой информации;
- разрабатывать и применять технологии обработки больших информационных потоков финансовой и экономической информации в режиме реального времени;
- структурировать информационные ресурсы в соответствии с их ценностью и полезностью, определять необходимость их защиты от несанкционированного доступа;
- работать с методической литературой и выработать управленческие решения в области информационной безопасности;

владеть :

- поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности;
- применения нормативных правовых документов в своей деятельности; - навыками работы с информацией из различных источников;
- навыками изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;

У обучающихся формируются следующие компетенции:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способность использовать нормативные правовые акты в профессиональной деятельности(ОПК-5);
- способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);
- способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);
- способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам вариативной части профессионального цикла (Б1.В.ДВ.10.1). Изучается на 4 курсе в 7 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 часов

Таблица 3.1 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54,1
Лекции	36
лабораторные занятия	-
практические занятия	18
экзамен	-
зачет	0,1
курсовая работа (проект)	не предусмотрено
расчетно-графическая (контрольная) работа	не предусмотрено
Аудиторная работа (всего):	36
в том числе:	
лекции	36
лабораторные занятия	0
практические занятия	18
Самостоятельная работа обучающихся (всего)	53,9
Контроль/экс (подготовка к экзамену)	-

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
-------	--------------------------	------------

1	2	3
1.	Структура службы информационной безопасности	Общая структурная схема службы защиты информации. Основные направления деятельности СУИБ
2.	Функции основных групп службы безопасности	Группа режима. Группа охраны и сопровождения. Техническая группа. Детективная группа. Должностные обязанности Минимальный штатный состав СБ и обязанности сотрудников
3.	Цели и задачи службы информационной безопасности	Цели обеспечения безопасности предприятия. Задачи службы Функции СИБ
4.	Организационные основы и принципы деятельности службы информационной безопасности	Организация деятельности службы безопасности Правовое обеспечение службы. Принципы организации службы. Гарантии безопасности объектов защиты Пакет документов для СИБ
5.	Лицензирование видов деятельности службы безопасности.	Лицензирование видов деятельности службы безопасности предприятия
6.	Управление службой защиты информации.	Методы управления СБП Функции процессов управления Функции процессов управления Методы управления Принципы управления СБП. Виды обеспечения деятельности СБП. Управление безопасностью предприятия в кризисных ситуациях
7.	Организация информационно-аналитической работы.	Цели и задачи информационно-аналитической работы. Направления и методы аналитической работы Этапы выполнения информационно-аналитических исследований производственных ситуаций. Методы выполнения аналитических исследований
8.	Организация работы с персоналом предприятия.	Подбор и подготовка кадров. Проверка персонала на благонадежность. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией

Таблица 4.2– Содержание дисциплины и ее методическое обеспечение

№ п/ п	Раздел (тема) дисциплины	Виды деятельности			Учебно- методич еские материа лы	Формы текущего контроля успеваемо сти (по неделям семестра)	Компетенции
		лек., час	№ пр.	№л лб.			
1	2	3	4	5	6	7	8
1.	Структура службы информационной безопасности	4			У-1 МУ-4	С	ОК-4, ОПК-5, ПК-10, ПК-15
2.	Функции основных групп службы безопасности	4			У-1,2, МУ-4	С	ПК-10, ПК-15
3.	Цели и задачи службы информационной безопасности	4	1		У-1,3 МУ-1,4	С,Т	ПК-8, ПК-10,

1	2	3	4	5	6	7	8
4.	Организационные основы и принципы деятельности службы информационной безопасности	4			У-1,4 МУ-4	С, Т	ОК-4, ОПК-5, ПК-8, ПК-15
5.	Лицензирование видов деятельности службы безопасности.	4	2		У-2,3 МУ-2,4	С	ОК-4, ОПК-5, ПК-8, ПК-10, ПК-15
6.	Управление службой защиты информации.	8	3		У-1,2,3 МУ-3,4	С	ОК-4, ОПК-5, ПК-8, ПК-10, ПК-15
7.	Организация информационно-аналитической работы.	4			У-2-6, МУ-4	С	ОК-4, ОПК-5, ПК-15
8.	Организация работы с персоналом предприятия.	4			У-1,3,4, МУ-4	С	ОК-4, ОПК-5,

С – собеседование.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические работы

Таблица 4.3 – Практические занятия

№	Наименование практической работы	Объем, час.
1.	Анализ заданного нормативно-правового акта Российской Федерации	6
2.	Работа с нормативно-правовыми документами	6
3.	Система анализа рисков и проверки политики информационной безопасности предприятия	6
Итого		18

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Структура службы информационной безопасности	1-2 неделя	6
2.	Функции основных групп службы безопасности	3-4 неделя	6
3.	Цели и задачи службы информационной безопасности	5-6 неделя	8
4.	Организационные основы и принципы деятельности службы информационной безопасности	7-8 неделя	8
5.	Лицензирование видов деятельности службы безопасности.	9-10 неделя	6
6.	Управление службой защиты информации.	11-14 неделя	7,9
7.	Организация информационно-аналитической работы.	15-16 неделя	6
8.	Организация работы с персоналом предприятия.	17-18неделя	6

Итого	53,9
-------	------

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_ib/index.php);

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

- путем разработки вопросов к экзамену

- методических указаний к выполнению практических работ.

типографией университета

- путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. № 301 по направлению подготовки 10.03.01 «Информационная безопасность» реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, 27,2 процента от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы №1 «Анализ заданного нормативно-правового акта Российской Федерации».	Разбор конкретных ситуаций	3
2.	Выполнение практической работы №2 «Работа с нормативно-правовыми документами».	Разбор конкретных ситуаций	3
3.	Выполнение практической работы №3 «Система анализа рисков и проверки политики информационной безопасности предприятия»	Разбор конкретных ситуаций	2
	Итого		8

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);		Организационное и правовое обеспечение информационной безопасности	Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Преддипломная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
Способность использовать нормативные правовые акты в профессиональной деятельности(ОПК-5)	Правоведение; Патентование;	Организационное и правовое обеспечение информационной безопасности	Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Преддипломная

			практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);		Основы риверсинжиниринга программных средств; Организационное и правовое обеспечение информационной безопасности; Технологическая практика; Проектно-технологическая практика; Методы защиты программного	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)		Организационное и правовое обеспечение информационной безопасности; Учебно-исследовательская работа студентов; Проектно-технологическая практика	Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Преддипломная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности		Организационное и правовое обеспечение информационной безопасности; Проектно-технологическая практика	Защита и обработка конфиденциальных документов; Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Защита выпускной квалификационной работы, включая

Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).			подготовку к процедуре защиты и процедуру защиты
--	--	--	--

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкал оценивания

Наименование компетенции	Критерии освоения		
	Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
ОК-4 - способность использовать основы правовых знаний в различных сферах деятельности	<p>Знать: Организацию судебных, правоприменительных и правоохранительных органов</p> <p>Уметь: использовать нормативно-правовые знания в различных сферах жизнедеятельности.</p> <p>Владеть навыками: Работы с нормативно-правовыми документами</p>	<p>Знать: правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности.</p> <p>Уметь: использовать нормативно-правовые знания в различных сферах деятельности.</p> <p>Владеть навыками: реализации и защиты своих прав</p>	<p>Знать: основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права.</p> <p>Уметь: использовать нормативно-правовые знания в нетиповых ситуациях.</p> <p>Владеть навыками: Правового анализа нормативных актов, регулирующих отношения в различных сферах жизнедеятельности.</p>
ОПК-5 - способность использовать нормативные правовые акты в профессиональной деятельности	<p>Знать: Организацию судебных, правоприменительных и правоохранительных органов</p> <p>Уметь: использовать нормативно-правовые знания в различных сферах жизнедеятельности.</p> <p>Владеть навыками: Работы с нормативно-правовыми документами</p>	<p>Знать: правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности.</p> <p>Уметь: использовать нормативно-правовые знания в различных сферах деятельности.</p> <p>Владеть навыками: реализации и защиты своих прав</p>	<p>Знать: основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права.</p> <p>Уметь: использовать нормативно-правовые знания в нетиповых ситуациях.</p> <p>Владеть навыками: Правового анализа нормативных актов, регулирующих отношения в</p>

			различных сферах жизнедеятельности.
ПК-8 - способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать: номенклатуру организационно-распорядительной документации службы информационной безопасности Уметь: сопоставлять организационно-распорядительную документацию с функциями службы информационной безопасности; Владеть навыками: Работы с технической документацией;	Знать: состав организационно-распорядительной документации службы информационной безопасности Уметь: сопоставлять ОРД требованиям нормативных документов Владеть навыками: Формулирования отдельных положений ОРД;	Знать: назначение и правовые основы отдельных положений организационно-распорядительной документации службы информационной безопасности Уметь: сопоставлять ОРД актуальной структуре предприятия; Владеть навыками: Формирования ОРД
ПК-10 - способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартам в области информационной безопасности	Знать: общие принципы лицензирования и сертификации в области ИБ Уметь: определять перечень действий для проведения анализа ИБ Владеть навыками: Участия в анализе требований регуляторов в области ИБ;	Знать: порядок проведения лицензирования и аттестации Уметь: определять несоответствия между текущим состоянием объекта информатизации и требованиями регуляторов в области ИБ; Владеть навыками: Анализа информационных систем на предмет соответствия нормативно-правовым документам	Знать: требования к лицензиатам и сертифицированным объектам Уметь: сопоставлять текущую структуру предприятия требованиям регуляторов в области ИБ; Владеть навыками: Формирования программ лицензирования и сертификации;
ПК-15 - способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ РФ, ФСТЭК	Знать: порядок формирования службы защиты информации на предприятии Уметь: работать с нормативными документами регуляторов в области информационной безопасности Владеть навыками: анализа нормативных требований регуляторов	Знать: требования к обеспечению функционирования службы защиты информации. Уметь: проектировать технологический процесс обеспечения информационной безопасности. Владеть	Знать: полный перечень действий по созданию службы защиты информации. Уметь: проектировать и реализовывать технологический процесс обеспечения информационной безопасности на предприятии;

		навыками: составления проектов организации службы защиты информации;	Владеть навыками: организации службы защиты информации
--	--	--	---

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология форматирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Структура службы информационной безопасности	ОК-4, ОПК-5, ПК-10, ПК-15	Лекция, СРС	Собеседование	1-4	Согласно табл. 7.2
2	Функции основных групп службы безопасности	ПК-10, ПК-15	Лекция, СРС,	Собеседование	1-8	Согласно табл. 7.2
3	Цели и задачи службы информационной безопасности	ПК-8, ПК-10	Лекция, СРС, практическая работа	Собеседование, тест	1-3	Согласно табл. 7.2
				Контрольные вопросы к ПР №1		
4	Организационные основы и принципы деятельности службы информационной безопасности	ОК-4, ОПК-5, ПК-8, ПК-15	Лекция, СРС, практическая работа	Собеседование,	1-7	Согласно табл. 7.2
				Тест		
5	Лицензирование видов деятельности службы безопасности	ОК-4, ПК-8, ПК-10, ПК-15, ОПК-5, ПК-10,	Лекция, СРС	Собеседование		Согласно табл. 7.2
				Контрольные вопросы к ПР №2		

6	Управление службой защиты информации.	ОК-4, ОПК-5, ПК-10, ПК-15	Лекция, СРС, практическая работа	Собеседование	1-9	Согласно табл. 7.2
				Контрольные вопросы к практической №3		
7	Организация информационно-аналитической работы.	ОК-4, ОПК-5, ПК-15	Лекция, СРС	Собеседование	1-7	Согласно табл. 7.2
8	Организация работы с персоналом предприятия.	ОК-4, ОПК-5, ПК-8	Лекция, СРС	Собеседование	1-8	Согласно табл. 7.2

Примеры типовых контрольных заданий для текущего контроля Вопросы для собеседования

Тема 7. Организация информационно-аналитической работы.

1. Цели и задачи информационно-аналитической работы
2. Задачи, возникающие при выполнении информационно-аналитической работы
3. Направления и методы аналитической работы
4. Что включает в себя такое направление, как обнаружение каналов несанкционированного доступа к информации?

Тесты для промежуточного контроля знаний

Тема 4. Организационные основы и принципы деятельности службы информационной безопасности.

1. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта
 - Группа режима
 - Группа охраны и сопровождения
 - Техническая группа
 - Детективная группа
2. В обязанности какого сотрудника входит разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранности данных
 - Сотрудник группы безопасности
 - Администратор безопасности системы
 - Администратор безопасности данных
 - Руководитель группы
3. В обязанности какого сотрудника входит контроль за выполнением плана восстановления после инцидента информационной безопасности
 - Сотрудник группы безопасности
 - Администратор безопасности системы
 - Администратор безопасности данных
 - Руководитель группы

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулирующих следующими нормативными актами университета:

- Положение П 02.016 – 2015 «О балльно-рейтинговой системе оценки качества освоений образовательных программ»;

- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение практической работы №1 «Анализ заданного нормативно-правового акта Российской Федерации».	8	Выполнил, но «не защитил»	10	Выполнил и «защитил»
Выполнение практической работы №2 «Работа с нормативно-правовыми документами».	8	Выполнил, но «не защитил»	10	Выполнил и «защитил»
Выполнение практической работы №3 «Система анализа рисков и проверки политики информационной безопасности предприятия»	8	Выполнил, но «не защитил»	12	Выполнил и «защитил»
СРС	0		16	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Итоговый контроль – зачёт в форме компьютерного тестирования : студенту предлагается 20 вопросов по различным темам курса из 5 категорий сложности. Вопросы 1-й категории сложности оцениваются в 1 условный балл, 2-й – в 2 условных балла, и т. д. В каждом вопросе один правильный ответ. Полученную итоговую сумму условных баллов (максимум 60) переводят в баллы на экзамене (максимум 36) путём умножения на 0.6 и округления до целого значения.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Аверченков, В. И. Служба защиты информации: организация и управление [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стереотип. - М. : Флинта, 2016. - 186 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=93356>
2. Литвак, Б. Г. Разработка управленческого решения [Текст] : учебник для студ. вуз. / Б. Г. Литвак. - М. : Дело, 2000. - 392 с.
3. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс] : учебное пособие / В. А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - М. : Издательский дом Высшей школы экономики, 2015. - 574 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=440285>
4. Степанова, Е. Е. Информационное обеспечение управленческой деятельности [Текст] : учебное пособие / Е. Е. Степанова, Н. В. Хмелевская. - М. : Форум, 2004. - 154 с.

8.2 Дополнительная литература

1. Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=93245>
2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : <http://biblioclub.ru/index.php?page=book&id=276557>
3. Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с.
4. Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с.
5. Петренко, В. И. Теоретические основы защиты информации [Электронный ресурс] : учебное пособие / В. И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. — Режим доступа: <http://biblioclub.ru/index.php?page=book&id=458204>
6. Ярочкин, В. И. Безопасность информационных систем [Текст] / В. И. Ярочкин. - М. : Ось-89, 1996. - 320 с.

8.2 Перечень методических указаний

- 1) Анализ заданного нормативно-правового акта Российской Федерации: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: В.В. Карасовский, О.А.Демченко. Курск, 2017.- 6 с.
- 2) Система анализа рисков и проверки политики информационной безопасности предприятия : методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: В.В. Карасовский, О.А.Демченко. Курск, 2017.- 9 с.
- 3) Работа с нормативно-правовыми документами: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: В.В. Карасовский, О.А.Демченко. Курск, 2017.- 11 с.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- 1) Федеральная служба безопасности [официальный сайт]. Режим доступа: <http://www.fsb.ru/>
- 2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: <http://fstec.ru/>
- 3) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: <http://biblioclub.ru>
- 4) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: <http://www.consultant.ru>
- 5) Научно-информационный портал ВИНТИ РАН [официальный сайт]. Режим доступа: <http://www.consultant.ru/>
- 6) База данных "Патенты России"
- 7) Аналитический раздел компании «Код Безопасности» <https://www.securitycode.ru/documents/analytics/>

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Организация и управление службой защиты информации» являются лекции и практические работы. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические работы, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практической работе предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Организация и управление службой защиты информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немислима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Организация и управление службой защиты информации» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Организация и управление службой защиты информации» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016. Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/1 7" TFT E700 (6 шт)